Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2009-09

No dark corners : defending against insider threats to critical infrastructure

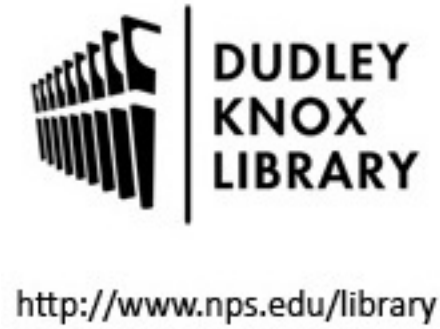
Catrantzos, Nicholas.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/4656

Copyright is reserved by the copyright owner.

Downloaded from NPS Archive: Calhoun



http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NO DARK CORNERS:
DEFENDING AGAINST INSIDER THREATS TO CRITICAL INFRASTRUCTURE

by

Nicholas Catrantzos

September 2009

Thesis Advisor: David Tucker
Second Reader: David Brannan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE No Dark Corners: Defending Against Insider Threats to Critical Infrastructure	5. FUNDING NUMBERS
6. AUTHOR(S) Nicholas Catrantzos	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government or the Metropolitan Water District of Southern California.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

An adversary who makes a frontal attack can be anticipated or repulsed. An adversary who attacks from within, however, cannot be so readily countered. This study intends to identify defenses against trust betrayers targeting critical infrastructure. Using a Delphi method, the study develops insights of experts from more mature arenas of defense against insider threats, such as workplace violence and counter-espionage, in order to assist infrastructure stewards with defending against the insider threat to critical infrastructure.

The findings uncover flaws in institutional defenses that adversaries can exploit, with infiltrators posing a greater threat than disgruntled insiders. Resulting recommendations run counter to accepted wisdom. These recommendations shape the contours of a No Dark Corners approach that applies and extends seminal theories of Newman's Defensible Space and Kelling's Fixing Broken Windows.

No Dark Corners replaces a laser for a flashlight. The laser is a narrow beam of workplace monitoring only by corporate sentinels, or security specialists. The flashlight is a broader beam of employee engagement and monitoring on the front lines at the team level. There are no easy answers. No Dark Corners shows promise in filling the gaps in traditional insider defenses to deliver the victory of ownership over surprise.

14. SUBJECT TERMS Critical infrastructure protection, insider threat, trust betrayers, infiltrators, disgruntled insiders, Defensible Space, Fixing Broken Windows, employee engagement, No Dark Corners.	15. NUMBER OF PAGES 105
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NO DARK CORNERS:
DEFENDING AGAINST INSIDER THREATS TO CRITICAL INFRASTRUCTURE

Nicholas Catrantzos
Security Manager, Metropolitan Water District of Southern California
B.A., University of California, Riverside, 1977

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: Nicholas Catrantzos

Approved by: David Tucker
Thesis Advisor

David Brannan
Second Reader

Harold A. Trinkunas
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

An adversary who makes a frontal attack can be anticipated or repulsed. An adversary who attacks from within, however, cannot be so readily countered. This study intends to identify defenses against trust betrayers targeting critical infrastructure. Using a Delphi method, the study develops insights of experts from more mature arenas of defense against insider threats, such as workplace violence and counter-espionage, in order to assist infrastructure stewards with defending against the insider threat to critical infrastructure.

The findings uncover flaws in institutional defenses that adversaries can exploit, with infiltrators posing a greater threat than disgruntled insiders. Resulting recommendations run counter to accepted wisdom. These recommendations shape the contours of a No Dark Corners approach that applies and extends seminal theories of Newman's Defensible Space and Kelling's Fixing Broken Windows.

No Dark Corners replaces a laser for a flashlight. The laser is a narrow beam of workplace monitoring only by corporate sentinels, or security specialists. The flashlight is a broader beam of employee engagement and monitoring on the front lines at the team level. There are no easy answers. No Dark Corners shows promise in filling the gaps in traditional insider defenses to deliver the victory of ownership over surprise.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

I am indebted to three groups for breathing life into this thesis.

THE DOCTORS: Lauren Wollman guided topic selection, research methodology, and identification of the best thesis advisers. Chris Bellavita counseled against tentative research topics whose pursuit he judged would become a forced march to music I could not stand for a year of exploration. Then came David Tucker, with gimlet-eyed scrutiny and painstaking attention to detail. He salvaged the research vessel when it was taking on water and navigating rough seas churned by time constraints and apparent contradictions. Finally, Dave Brannan offered refinements and field truth to pilot the thesis vessel to dry land and safe harbor.

THE GENTLEMEN OF THE SHADE: The Delphi process masks their identities. Just as Shakespeare's Falstaff alludes to unseen collaborators by this label, so must I recognize the generous souls of both intellect and hard-won scar tissue who stuck with me through three rounds of Delphi questions. They supplied unique, in-depth insights that produced the research findings, laying claim not only to my thanks but also to my admiration.

THE ENABLERS: Tom Goff, sensei and friend, magazine editor and corporate executive, scholar and crisis manager, was the best of sounding boards. Over a year of Saturday morning coffees, he supplied clarity and ideas through Socratic dialogue and trenchant debate. This infusion made it possible to part with extraneous ballast that would have otherwise ruined the voyage. Finally, Marilyn Frances, the superlative enabler, fairest of the fair, and Director of Life Support of Casa Catrantzos, swept away distractions with a steady fusillade of encouragement. Her optimistic pointers to a light at the end of the tunnel supplied the beacon to see the voyage through dark moments and fog advisories. A thousand thanks for a myriad saves, smiles, and nudges. You are the light that makes my day.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM, DEFINITIONS, AND CONVENTIONAL WISDOM

An adversary who makes a frontal attack can be anticipated or turned back with countervailing force. An adversary who attacks from within, however, cannot be so readily anticipated, nor defeated by force alone. As a 2008 report to the President explained, this is the insider threat problem for critical infrastructure:

> Essentially, the threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals cover a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate. (Noonan & Archuleta, 2008, p.32)

The overall intent of this study is to deliver countermeasures that critical infrastructure defenders can use to prevent terrorist attacks against the United States via insider threats and thereby reduce the vulnerability of America's critical infrastructure.

Throughout this study, **insider threat** means an individual, and more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust with the infrastructure or institution being targeted.[1] **Hostile** or **malicious insider** and **trust betrayer** also refer to the individual who represents an insider threat, although these two terms focus more attention on the individual than on the phenomenon. **Infiltrator** refers to a subset of hostile insider who sees himself or herself as an adversary prior to attaining insider status within the targeted infrastructure or institution. The infiltrator joins a targeted employer or group under false pretenses as a means of obtaining

[1] This definition anticipates and is supported by a research finding described at greater length later in the study.

sufficient access to facilitate an attack. **Recruited asset,** in the context of an insider threat, refers to an individual already occupying a position of trust who can be induced or manipulated to act against the institution to either carry out an infrastructure attack or provide information to support such an attack. **Institutions** refer to public and private sector enterprises, employers, entities, and organizations, particularly those that operate critical infrastructure. **Corporate sentinels** refers to the functions and employees in an institution whose job it is to perform security functions, including watching over people and assets on behalf of the institution. Finally, **No Dark Corners** is shorthand for an array of defenses centering on a strategy that configures the job to reduce chances for a sole individual occupying a sensitive area undetected; another trusted employee must be within line of sight or some form of remote surveillance or detection must create the possibility that someone may be watching. Additionally, **No Dark Corners**, writ large, broadly refers to the suite of defenses that stand in contrast to the conventional wisdom on how to counter the insider threat and that form the ultimate recommendations of this thesis.

Other, more conventional terms apply to the accepted wisdom for addressing insider threats: **random audits**, **background investigations**, **technologically based monitoring**, and traditional reliance on a security force or other assigned **corporate sentinels** to exercise the organization's responsibility for insider threat defense. Random audits may be financial or operational checks for unexplained anomalies that could give away a hostile insider. Background investigations, particularly the pre-employment variety, are intended to detect the same kind of anomalies in time to bar insider access. Technologically based monitoring consists of electronic audit trails, such as remote or automated surveillance of operations and the people who carry them out, such as access to networks, control systems, and to places or assets equipped with surveillance cameras, alarms, or access control devices. Corporate sentinels are the institution's designated watchers. They include the traditional members of a security staff, information technology specialists

monitoring electronic mail and other automated systems, and other people and functions in an institution who are assigned official roles of oversight. As the research will show, even expert defenders resort to conventional measures such as these with the confidence that they can defeat the insider threat. Yet, on further scrutiny, the same experts who champion such countermeasures find that they could readily bypass them, if the tables were turned and they themselves were tasked with carrying out an insider attack. Out of this apparent contradiction, this study creates a new model under the banner of No Dark Corners. This model accounts for the apparent contradictions and offers a different method of dealing with the insider threat.

B. RESEARCH OBJECTIVES

The primary research objective is to identify countermeasures that reveal trust betrayers and actions that defenders can deploy within existing resources at their disposal. This process involves applying lessons of experts from more mature arenas of defense from insider threats, such as workplace violence, line management, corporate security, and counter-espionage, in order to assist infrastructure stewards with early identification and timely containment of the insider threat to critical infrastructure.

The secondary research objective is to discern possible innovations of strategic value. In other words, if current indicators and countermeasures fall short, what should we do differently?

C. BACKGROUND AND LIMITATIONS

This study deals with a statistically rare phenomenon, as informed observers have found that trust betrayal is statistically infrequent (Shaw & Fischer, 2005). In keeping with the greater, homeland security aim of reducing America's vulnerability to terrorist attacks on critical infrastructure, this study is not about thieves, inept employees, embezzlers, or others whose deeds may pose an incidental threat. Nor is it about post-loss event investigations or low-level policing activities that any institution's security force carries out in the

course of defending the organization's interests and assets. Finally, since there can be no treason if there is no corresponding betrayal of trust and violation of loyalty (Ben-Yehuda, 2001, pp. 307–308), remote hackers and typical cyber intruders also fall outside the purview of this study. Instead, the focus remains on countering trust betrayers, or hostile insiders, through real-world, actionable strategies.

If, as the literature suggests, a "miniscule fraction" of the people in a position to betray trust actually do so (Eoyang, 1994, p. 80), then quantitative methods will not avail in addressing the research objectives of uncovering practical countermeasures and strategic innovations. Under the circumstances, an iterative process for collecting and distilling judgments of experts offers more promise in such circumstances, hence, the appeal of the Delphi method's advantages (Skulmoski, G. J., Harman, F. T., & Krahn, J., 2007).

With homeland security being a relatively new field of endeavor (Shaw & Fischer, p. iii)[2] in the United States and critical infrastructure protection a subset that did not emerge as a national priority before 1998,[3] there exists no discipline-specific body of experts on the insider threat to critical infrastructure per se. Even those experts assembled to study the cyber aspect of the larger insider threat have admitted limitations of the cyber-centric approach in terms of instituting effective countermeasures. For example, two experts have claimed, "we need multidisciplinary research teams (not just *geeks*) investigating what we should look for as indicators of possibly malevolent behavior (Brackney & Anderson, p. 14).

Efforts to develop predictive models for detecting and interdicting malicious insiders have ranged from a quantitatively based yet unproven formula (Puleo, 2006) to broad-based theoretical models designed mainly to predict the

[2] In their preface, Shaw & Fischer (2005) acknowledge that they have long studied insider espionage, but the insider threat, as it relates to international terrorism, "is only now emerging."

[3] This was the year of the release of Presidential Decision Directive 63, which published the findings of the President's Commission on Critical Infrastructure Protection.

triggers that lead an assassin or radical group to take violent action (Fein & Vossekuil, 1998; Olson, 2005). The literature contains much analysis on the psyches (Kaupla, 2008; Shaw & Fischer, 2005), social climates (Ben-Yehuda, 2001), and cyber vulnerabilities (Noonan & Archuleta; Kowalski, Cappelli & Moore) associated with malicious insiders. Yet, analysis appears more limited on pragmatic lessons and inferential guidance that apply directly to practical countermeasures. However, research on threats from assassins to saboteurs suggests that applicable findings may be adaptable from indirectly related works and may offer more promise in charting a course to defending against the malicious insider who is more dangerous than a computer hacker (Fein & Vossekuil; Olson; U.S. Congress OTA, 1990).

D. APPROACH

In this context, it stands to reason that defense against the insider threat to critical infrastructure would benefit from lessons adapted from more mature disciplines, such as counter espionage, prevention of workplace violence, and defense against systemic institutional fraud. Insider threats in these disciplines meet the same general definition of insider threats to critical infrastructure, i.e., a person or persons with access or knowledge of an organization and the motivation or intent to cause harm or adversely affect the organization's mission.[4]

If these other disciplines have the potential to inform the study of insider threats to critical infrastructure, it follows that subject matter experts from such disciplines, who themselves have long and direct experience in identifying, investigating or countering the adverse effects of insider threats, also possess insights useful for advancing a deep understanding of the insider threat phenomenon. This study, therefore, adopts the qualitative approach of the Delphi method to derive insights and judgments from a diverse group of experts

[4] This insider threat definition draws on common elements expressed by Noonan & Archuleta (p. 5) and Brackney & Anderson (p. 63). The latter also make a point of defining the malicious insider in terms of having access, regardless of whether that access is legitimate. Thus, in Brackney & Anderson's view, a janitor who has access to a sensitive facility but is not authorized to do more than clean it may still be considered an insider.

who did not interact directly and supplied their evaluative thoughts independently, thereby avoiding groupthink or undue influence of dominating personalities.

Through a series of questions, answers, analysis, and feedback, the Delphi panelists supplied insights that at first validated the accepted wisdom on insider threat defense, including endorsement of random audits, background investigations, and technologically based monitoring. However, as the Delphi inquiries progressed, the same experts ultimately came to identify flaws in these defenses that, in turn, laid the foundation for the No Dark Corners strategy that this thesis recommends as an alternative to the accepted wisdom.

E. METHODOLOGY

Delphi respondents were selected based on having previously demonstrated "deep smarts" insight "based more on know-how than on facts; it comprises a system view, as well as expertise in individual areas (Leonard & Swap, 2004). In addition to at least 20 years of involvement in critical infrastructure protection, crisis management, espionage, workplace violence, failure analysis, or complex fraud investigations, each Delphi respondent has career experience that included employment in or oversight of employees in the private sector.[5]

Table 1 presents a general description of the individual expertise of the respondents. Many of the individuals have overlapping areas of expertise, but this table focuses on the main skill sets that led to their invitation to form this Delphi group. The reason Table 2 omits some overlapping expertise is that too much detail on each expert's capacity would reveal identities. Consequently, Table 2 represents a fuller picture of the range of talents that this Delphi dozen possess, without compromising their confidentiality.

[5] Since 85% of critical infrastructure is considered to be in the hands of the private sector (Lewis, 2006), representation of the private sector is important to this study.

Table 1. Individual Expertise of Delphi Group Members

Expert 1	Case officer for two different U.S. government agencies. Recruited agents in foreign countries. Investigated fraud in private sector.
Expert 2	Chief executive and expert in uncovering collusive networks and in managing private sector collaboration with law enforcement and prosecuting agencies.
Expert 3	Senior investigator with global due diligence firms. Investigative journalist specializing in complex international fraud cases.
Expert 4	Ombudsman for major police force. Chief of detectives. Former military policeman.
Expert 5	Critical infrastructure security director. Former undercover agent of federal law enforcement agency.
Expert 6	Former case officer recruiting agents for U.S. in third world countries.
Expert 7	U.S. counterintelligence officer debriefing traitors.
Expert 8	Corporate executive and systems integrator for defense business formerly involved in development of intelligence platforms.
Expert 9	Career investigator, business owner specializing in uncovering complex corporate fraud.
Expert 10	Corporate executive, corporate communications specialist and crisis management adviser.
Expert 11	Critical infrastructure operations director involved in leading agency response to and recovery from major natural disaster.
Expert 12	Clinical psychologist specializing in workplace and domestic violence prevention, assessment, and response.

Table 2. Composite Expertise of Delphi Group Members

Professional Expertise	Experts Possessing Expertise
Interaction with hostile people and organizations	12
Critical infrastructure protection, management	5
Corporate fraud investigations	5
Public or private sector undercover operations	4
Organizational response to international threats	4
Response to threats as a police or military professional	4
Workplace violence case management responsibility	4
Crisis communications and response	3
Executive with profit and loss responsibility	3

Each Delphi round involved transmitting questions by e-mail and responding by return e-mail with at least two weeks between rounds. All respondents agreed to participate in the study under standard confidentiality protections and with repeated reminders that no classified or proprietary information was being solicited for the study. Of the dozen experts who agreed to participate in three rounds of Delphi surveys, 100% saw the process through from start to finish.

1. Delphi Round 1

The first round of Delphi questions consisted of level-setting questions to begin seeking a common definition of the insider threat and its observable dimensions. Round 1 encouraged respondents to review their own experiences to reconstruct case histories. From these case histories, respondents reported

on what caused trust betrayers to be exposed and what signs pointed the way to the exposure. Appendix A presents the specific questions for Rounds 1, 2, and 3.

The objective of leading with the Round 1 questions was to ease into thematic content while seeking points of convergence without superimposing foreordained conclusions.

Using this loosely structured combination of easy questions also encouraged participation and allowed using a textual analysis tool to seek out non-obvious points of convergence, to be discussed further in Chapter II.

2. Delphi Round 2

The second round of Delphi questions was more complex and the most demanding of the Delphi surveys. It included feedback from Round 1 and asked the experts to comment on the extent to which they agreed with results from the earlier round. Round 2 also presented more narrative questions, before concluding with a series of scenario questions presenting two archetypal trust betrayers whose descriptions reflected composites of insider threats discussed in Round 1. Related questions asked the respondents to predict which composite insider would be more likely to carry out what kind of attack and to match trust betrayers relative to a given attack scenario. The questions from Round 2 appear in Appendix A, and the feedback that accompanied these questions for the benefit of the respondents is in Appendix B.

By feeding expert input back to the respondents, Delphi Round 2 created an opportunity for validation and rejection of ideas captured in Round 1. It also created an opportunity to capture points of expert convergence and divergence visually through a series of pie charts highlighting areas of strong agreement and wide variation.

3. Delphi Round 3

Finally, the last round played back to the experts their collective responses from Round 2. It then shifted gears. Delphi Round 3 now took the experts out of their customary roles as defenders and cast them as adversaries tasked with carrying out an attack against critical infrastructure. Round 3 asked respondents to select a Level 1 critical infrastructure to attack and decide whether to do so by recruiting a disgruntled employee already possessing access to the target or, instead, rely on infiltrating one's own agent. Appendix A, once more, shows the questions that formed Delphi Round 3.

F. SUMMARY

With the selection of the Delphi methodology, identification of a dozen experts to make up the Delphi respondent pool, and formulation of questions to explore the insider threat, all that should now remain would be to harvest insights and distill them into new, actionable knowledge for the advancement of homeland security efforts to defend critical infrastructure. As the next chapter will show, however, the results were varied, and in some cases, even contradictory from one round to the next.

II. RESULTS

A. DELPHI ROUND 1: EXPLORING THE PROBLEM

Round 1 responses diverged widely, as Table 3 shows. Each column contains a different expert's answers to questions across the grey row. Highlighted text marks items emphasized or illustrated in case studies that respondents offered. Bold lettering within the highlighted text reflects additional emphasis from the experts through either repetition or greater priority within respondent comments. Italics reflect direct quotes experts used for emphasis.

Table 3. Delphi Round 1 Response Compilation

E#	1-Definition/ Categories	2-Observable Tactics	3-Actions/ Motives	4-Exposed By	5-Signs	Misc. Remarks
1	An in-place asset. Those who leak, back stabbers, saboteur out to destroy, whistle-blowers, supporters of hostile outsiders, and professional conspirators.	Worked long hours, abused position to pay for gambling debts. Road rage arrest. Character assassination campaign(s) against co-workers perceived as threats or competitors.	Betrayed other individuals and organization for *self-aggrandizement* or out of resentment, revenge.	Due diligence checks including licenses, investigation of allegations made by spouses, routine audits.	External reports of irregularities and follow-up investigations into same.	***Ideology** may play a **lesser role in corporate** cases **but** is **primary in a terrorist scenario**.*
2	Individual, group, or organization using a position of trust or power to advance an agenda at the expense of the larger group. Employee having a grudge; religious (leader)/politician abusing position for enrichment or gratification; lobbyist for enrichment.	Arrogance, as if above rules and laws. Displays of ego, including in hobbies. Viciousness and intimidation in attacking other insiders or outsiders who raise questions that could expose hostile insider.	Aggressive threats of legal action and filing of lawsuits as intimidation tactic/Suppress opposition or probes that could uncover improprieties	Own arrogance and overcon-fidence, resulting in failure to cover tracks adequately; former victims coming forward with complaints; expert investigation.	*Constantly seeking power*	Hostile insider is generally *dismissive of victim(s)*
3	Employee who can damage/acts from incentive + opportunity	*"Beat the system" talk, behaviors*	Embezzlement and other fraud for financial gain	*Rumors and suspicions reported* to mgt and *then investigated*	Investigation confirming rumors and suspicions	*Greatest loss from insider at highest level*, particularly for financial damage.

E#	1-Definition/ Categories	2-Observable Tactics	3-Actions/ Motives	4-Exposed By	5-Signs	Misc. Remarks
4	Trust betrayer isolated because of *elitism* or *anger and aggression*	Elitism – *considers others inferior*. *Expressed hate and anger*. *Secrecy*. Paranoid survivalist with unauthorized weapons and ammunition.	Willful refusal to assist – payback. Coercion and self-dealing – greed. Altering records – *self-aggrandizement*.	Some audits and procedural reviews and inspections.	*Growing hostility*. Ultra conservatism. Consistent abusive or *unexplained anger*. Alcoholism. Gambling. Too much intensity, lack of humor.	Isolation is a critical aspect.
5	Threat from people with legitimate access	Seeking max influence or access in own purview to *reduce discoverability*.	Sabotaged equipment and called in threats, causing shutdown/Getting even after disciplined and before terminated.	Post-event investigation, logs showing suspicious after-hours access.	*Decline in* employee's *performance*. visible *anti-social behaviors*.	*"Sudden" anomalies usually have precursors that supervisors don't act on* out of lack of knowledge or fear of legal action and discrimination charges.
6	Harm from someone "friendly"/Disgruntled or infiltrator.	---	Getting even	Usually after the fact	---	*Getting even a central theme*; actual damage not necessary if intent is to disrupt.
7	Someone with equities in the employer organization; motivated by money, resentment, revenge, weakness, perceived "homeland" obligations, wish to "help" the mother land.	*Unexplained changes of personality, mood, or conduct*; unexplained money, family life, *outside associates*. "Beneath me" attitude. Difficulty with covert duties and lack of recognition.	Caused deaths without remorse. *Few motivated solely by money*. Rise of anti-American and anti-Western sentiments.	Co-worker raising concerns.	Defector or double agent may reveal insider. FBI sting operations.	*Every advance in technology creates new vulnerabilities*.
8	Person(s) in an org./*Sick fun*, spite, money, or treason.	Collusion with others.	Falsified documents for financial gain.	Random audit	Few signs in advance. Good auditing helps.	*Frequent rotations* of personnel a remedy, *good auditing* a must.

E#	1-Definition/ Categories	2-Observable Tactics	3-Actions/ Motives	4-Exposed By	5-Signs	Misc. Remarks
9	Anyone enjoying position of trust who is willing to harm organization. Can be principals, directors, employees, vendors or contractors. Financial gain most common, with relief from personal financial stress as the goal. Need for empowerment or revenge. *Whistle-blower*, rogue employee.	***Always exploits the organization's weakness.*** ***Deterred only by strong chance of discovery and swift punishment.*** *Insider is* ***never observed as a threat,*** employs *secrecy*, ***often the picture of the perfect employee***. Good audits would uncover but are either missing or perfunctory.	Exploited lax internal controls to embezzle; fraud by intimidating junior employees into silence; creating false business entities to submit false or inflated invoices; accepting bribes to breach trust. Rogue employee gambling entire organization to win back losses.	Unanticipated, in-depth audits, due diligence investigations.	Audits and supervisory oversight, use of monitoring systems.	Strong deterrence measures discourage every category of insider threat, raising potential of being discovered and of receiving real punishment.
10	Has access, intends harm/loner v conspirator; by target: individual, property, or system.	Hostile *conversational spillage/ inexplicably hostile behavior* or curiosity , questions/abnormal work hours.	Stealing personal info via data system and posting on Internet to embarrass company founder for perceived wrongs and from paranoia.	Discovery of results of actions, self-revelation by picketing workplace after filing of criminal charges.	Insider's ***own disclosure***.	Self-revelations a recurring feature.
11	Disgruntled worker, emotionally disturbed, union activist, opportunist seeking gain, zealot with a cause.	Loners, gun fanatics, secretive, avoiding eye contact even in casual conversation, quiet – except haters talk about hate, usually men.	Stealing/ financial gain.	Other employees and supervisors.	Good employees seeing something wrong and acting on it	***Persons who hate*** company or country are ***usual-ly outspoken about it***, but difficult to get rid of.
12	Individuals w/i an org who pose threats of violence or want to cause damage. Threats vs. supervision in general, disgruntled, whistle-blowers.	For cases of violence, *not sneaky but stewing in own myopic juices*. They focus on the individual. For sabotage and malicious whistle-blowers, build up to their action.	*Malicious whistle-blower slowly builds up a body of questionable documentation*, using signature words like "unfair" and "hostile workplace."	Peers, co-workers who bring unusual actions or behaviors to attention of managers.	Poor coping skills, portrays self as victim.	A shooter acts alone and is ***looking for relief*** and can often be guileless. An internal saboteur is ***looking for victory*** and builds up to an attack.

In Table 3, the first column, E, corresponds to the number assigned each expert in Table 1 of the preceding chapter, where the experts were first introduced by background and expertise. The numbered questions 1–5, which form the next series of columns, correspond to the main questions of Delphi Round 1 (available in their entirety in Appendix A). A final column captures miscellaneous remarks that the experts offered in the course of crafting their responses.

The highlighting, underscoring, and bold type drawing emphasis to words in Table 3 represent an attempt to focus on information already suspected of being of interest based on attention drawn by respondents, as opposed to unguided data mining. Thus, experts commented more on these items, offered cases illustrating these points, or did both. These areas of emphasis also aligned generally with literature on hostile insiders in the fields of workplace violence, espionage, and corporate fraud. As a result, these latter areas of emphasis were taken as representative of more indicative or common themes, hence, worthy of closer scrutiny—a method some analysts use for avoiding analytic overload (Hollywood, Snyder, McKay, & Boon, 2004, pp. xxi and 83).

Textual analysis using first the overall input and then the highlighted material helped uncover common themes in expert observations. Placing the first responses into a text cloud in Figure 2 made patterns more visually obvious.[6]

[6] This visual analysis of survey data came via http://www.tagcrowd.com at no cost for educational uses, thanks to Daniel Steinbock, a doctoral student at Stanford University. The output itself is called a text cloud, which is also called a tag cloud.

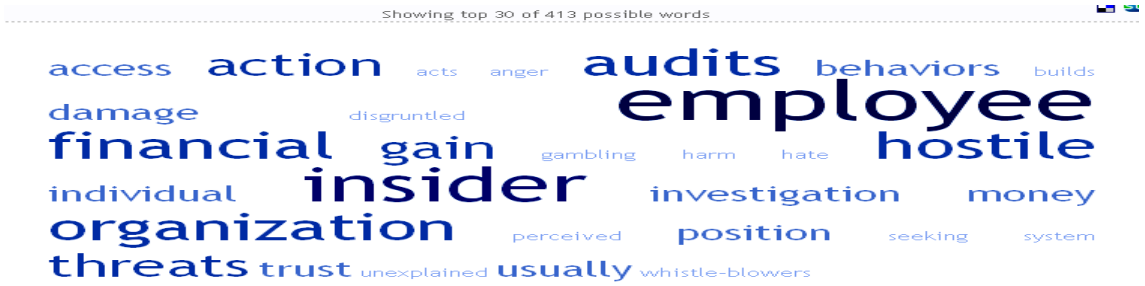


Figure 1. Text Cloud Showing Frequency of Words in Table 3

The words in Figure 1 appear in alphabetical order, but their size and relative emphasis tie directly to the frequency of their appearance in the unscripted responses. Thus, y experts used the term “employee” most often in their responses, then “insider” with “audits,” “financial,” “hostile,” and “organization” next ranking in frequency of appearance. This first text cloud compilation and sorting of overall responses, highlights observations and themes common to the insider threat writ large, i.e., the insider as an employee, often motivated by financial gain, operating in an organization, and subject to being given away by actions, audits, and behaviors.

To zero in on the more telling remarks of respondents and, in so doing, impart greater granularity to the first text cloud, the highlighted material from the response compilation (Table 3) next went into another text cloud sorting that yielded the results shown in Figure 2.

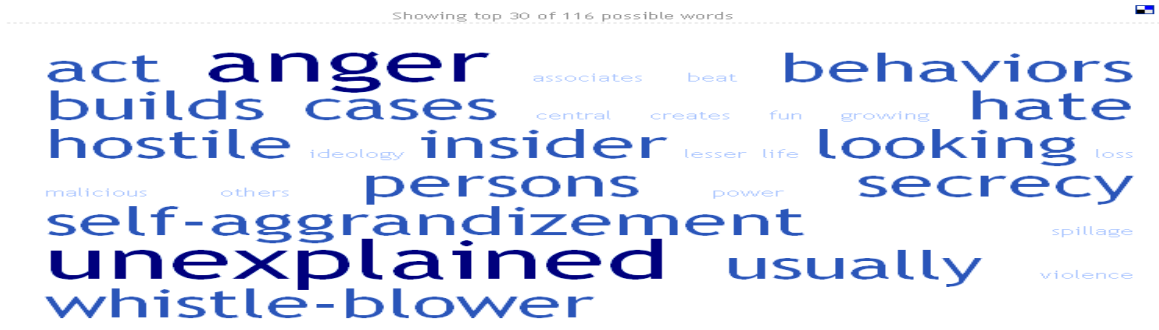


Figure 2. Text Cloud Showing Frequency of Words in Highlighted Items

The text cloud in Figure 2 brought more indicators to the surface. The most telling was unexplained anger, the two most prominent words. Other themes also emerged, such as tendencies of self-aggrandizement and secrecy among hostile insiders, which offer possibilities as indicators. A display of unexplained anger might, in itself, be insufficient to suggest the presence of a hostile insider. Taken together with other behavior, however, such as secrecy and a tendency to self-aggrandizement, some experts found this combination more indicative of a potential trust betrayer. Respondents with backgrounds in the worlds of corporate fraud investigations, intelligence, and clinical assessment of workplace violence threats independently converged on the notion that the malicious whistle-blower is becoming a less pernicious but more common hostile insider in the work place. However, as this employee has an axe to grind or a pocket to line, the malicious whistle-blower is unlikely to seek the total destruction of a targeted organization, rather than its humiliation or some form of compensation. Meanwhile, money and financial gain, which were prominent in Figure 1, were absent from Figure 2. One respondent indirectly offered the reason for this omission by noting that the most destructive damage is rarely driven purely by a desire for financial gain.

The text cloud analyses and two experts' categorizations of insider threats then helped formulate the basis for Delphi Round 2 inquiries.

Specifically, is there value in broadly categorizing insider threats in terms of whether they plan their attacks? Evidence of planning corresponds to the insight of a behaviorist respondent who noted that the saboteur's objective is seeking victory. By contrast, a dearth of planning that could instead present itself as an eruption corresponds to what the same respondent called the rage killer's objective of seeking relief. Pursuing such a distinction further would offer value in contrasting the different types of cases already cited by the respondents. It would also yield a simpler, more intuitive way of drawing distinctions and seeking corresponding behavioral signatures that could give away malicious insiders before they carry out their attacks. Thus, this new tentative categorization

formed the basis not only for further questions, but for formulation of two different kinds of insider threat scenario to structure respondent thinking along common denominators without pre-ordaining responses in the next round. Appendix B provides the summary of Delphi Round 1 findings that accompanied the questions that went to experts as Delphi Round 2 (viz. the Delphi Round 2 questions in Appendix A).

B. DELPHI ROUND 2: SHARPENING THE FOCUS

Delphi Round 2 played back the results of Round 1 for to the experts in an effort to seek calibration, and also furthered the exploration into indicators through a variety of approaches, including a series of scenario-based questions to see which of two types of hostile insider would pose a greater threat. Respondents received Appendix B to summarize the findings from their initial responses.

1. Overall Results of Round 2

Some themes invited strong expert convergence:

- Indicators of unexplained changes in behavior and in resentful or disgruntled presentation of the hostile insider.
- Secondary indicators of the hostile insider exercising overly proprietary interest in the job, expressing a perception of unfair treatment, and appearing arrogant or elitist.
- Random audit as a good, if not the best, countermeasure.
- The planner as the bigger threat to the institution, with some distinctions offered in remarks to the effect that a workplace violence attack, or rage killing, might constitute a personal tragedy for those victimized but was not an existential threat to the institution.

Other themes that showed early promise in surfacing useful distinctions for further probing failed to win strong or consistent support as indicators in the eyes of the Delphi experts.

- Does the hostile insider have a signature of withholding information? Respondents suggested that this might be true enough but was often difficult if not impossible to gauge until after the fact, hence of limited predictive value.
- Seeking power, being secretive, and exhibiting decline in performance also proved to be nonstarters. Clarifying comments explained that some of these traits were equally visible elsewhere, hence of limited value in trying to uncover hostile insiders. One respondent reasoned that ambitious competitors could easily seek power without becoming insider threats. Similarly, another respondent noted that, in his experience with traitors, once they had embarked upon a plan for stealing secrets to pass to a foreign power, they tended to level off in their outward ambitions and general performance. Evidently, this is to avoid inviting scrutiny while, at the same time, concentrate their energies on their clandestine endeavors.
- Efforts at categorization, whether as an insider seeking victory vs. relief, or as belonging to one of three classes (embezzler-thief, saboteur, or shooter (rage killer/workplace violence perpetrator) also failed to comprise a gravitational core to attract expert consensus. The very respondents who first suggested them negated some of these tentative categorizations. Evidently, there is just too much variation in views and in real cases to permit ready categorization along these lines.

2. Depictions of Convergent and Divergent Findings

Many of the results of Delphi Round 2 lent themselves to capture via spreadsheet or chart, hence, these at-a-glance summaries:

Table 4. Ratings of Insider Threat Observations

	Compact Version of Question	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
A	Definition			58%	42%
B	Beat the system	17%	42%	33%	8%
C	Secretive	8%	42%	17%	33%
D	Owns the job	8%	17%	58%	17%
E	Withholds info		33%	33%	33%
F	Arrogant, elitist	8%	25%	25%	42%
G	Unexplained changes		25%	33%	42%
H	Resentful		8%	67%	25%
I	"Perfect" employee	17%	42%	42%	
J	Getting even	8%	50%	42%	
K	Seeking power	33%	42%		25%
L	Says "unfair"		42%	50%	8%
M	Work declines	25%	42%	33%	

In Table 4, areas of strong convergence are highlighted in blue. Over 70% expert agreement or strong agreement is evident in responses associated with questions A, G, and H. The agreement is rated strongest for these three items because there was also no disagreement registered for any of them. Also highlighted in blue is a fourth item, D. However, while agreement here also exceeded 70%, there was 8% disagreement for the same category. Items highlighted in purple, however, reveal more divergence of expert views.

Visual depictions of the areas of convergence appear in Figure 3.

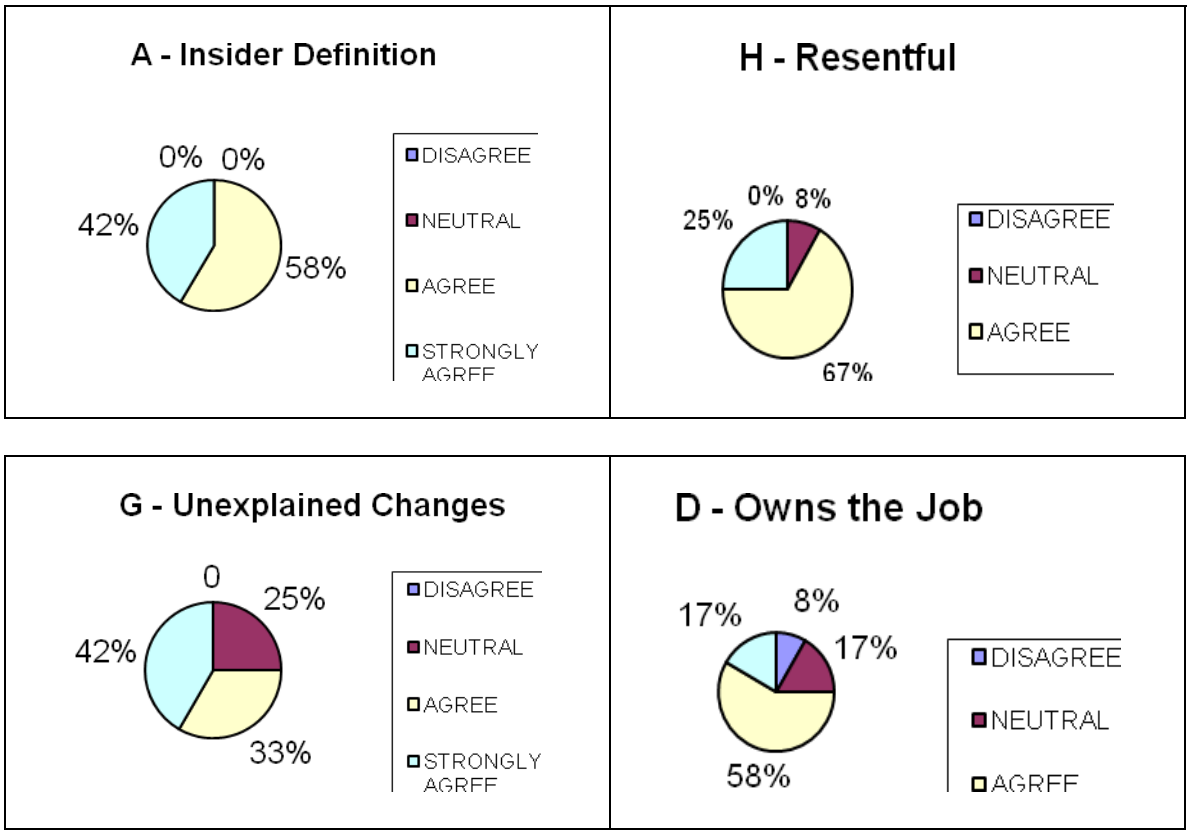


Figure 3. Areas of Convergence of Insider Threat Observations

The foregoing areas of convergence are strongest in yielding a shared understanding of the definition of an insider threat as an individual possessing legitimate access and occupying a position of trust in or with the organization targeted. In amplifying comments, Expert 11 noted that trust betrayers can be at all levels, from entry to top management. Expert 9 observed the need for a relationship to the target, which could have an insider being a vendor, as well as a director, rather than just a traditional employee. Finally, Expert 10 pointed out that the often-unremarkable member of a janitorial service could manage to gain insider access and move about unhindered because the custodial crew is virtually invisible in many organizations.

INDICATOR: **Unexplained changes** in personality, mood, or conduct were associated with trust betrayers by 75% of the Delphi experts. Of the remaining 25%, all registered as neutral. Expert 5 suggested that such changes are not always categorically ostensible. Expert 7, whose primary focus is

espionage, found in his experience that the majority of trust betrayers he encountered maintained a nondescript behavior pattern, often to mask hostile actions. Having recruited trust betrayers himself, Expert 1 commented that some hostile insiders were bilious by natural disposition, hence offering no additionally discernible indication of a threat by an examination of their conduct alone.

INDICATOR: Similarly, 92% of the experts agreed that the hostile insider may appear **resentful, disgruntled, or anti-social**. The remainder, registering as neutral, indicated that this is generally true but not necessarily always the case.

INDICATOR: Finally, while 75% agreed that the hostile insider is likely to demonstrate an **excessively proprietary interest in the job** (i.e., "owns the job"), diverging opinions from Expert 5 and Expert 6 noted that such an individual may intentionally seek to appear average in order to avoid drawing undue attention. Others, such as Expert 9 noted that the hostile insider involved in a demanding scheme would avoid taking vacations in order to constantly cover his tracks.

SUPPLEMENTAL INDICATORS: The Delphi experts diverged in the extent to which they rated these as potential indicators, with an emerging consensus that there is enough variation in cases of trust betrayers to make none of these dispositive by itself:

Withholding information. While 66% saw this behavior as indicative, 33% rated this as neutral. Expert 7 observed that it is hard to know what was withheld. Similarly, Expert 1 noted that those who withhold information eventually draw attention to themselves, which would be antithetical to a trust betrayer's objectives. Expert 12, on the other hand, saw this indicator as a matter of timing, where early on the hostile insider is very open but may then change as a result of not being heard. Expert 9 best accounted the reason for the variation in views on this potential indicator as being anomalous because indistinguishable, per se, from behavior of ambitious and competitive co-workers seeking advancement. Also, when used effectively as a tactic, it cannot be

readily gauged or identified, therefore, not strong enough to serve as a trapline when viewed in isolation. However, it may be useful as something to look for if other indicators are apparent.

Arrogant, elitist. Additionally 67% of the experts had observed arrogant or elitist behavior on the part of malicious insiders. Nevertheless, the trait was not seen as universal.

Experts did note that foregoing indicators should be viewed in combination with other signals, rather than in isolation, as potential signals of an anomaly worth probing further to evaluate its potential to blossom into an insider threat.

ADDITIONAL AREAS OF CONVERGENCE: Delphi respondents in this round also showed strong convergence in shared observations derived from Round 1 that were presented for review and assessment, as Figure 4 shows.

Figure 4 shows agreement of experts in certain areas with no disagreement whatever. By a two-to-one ratio, Delphi respondents recognized unexplained anger as a common indicator for insider threats. Where experts found this indicator subdued, it was concealed until after-the-fact where it surfaced in the course of debriefings. Expert 7, for example, explained that in espionage cases unexplained anger tends to be more muted or not displayed in order to mask clandestine activities because discovery is the trust betrayer's biggest existential threat. Expert 2 experienced cases where investigation revealed that the insider's anger was discernible but arguably justifiable, particularly if one digs deep enough. Experts 4 and 12 observed that anger on the part of a malicious insider may not be so much unexplained as out of proportion to the situation and circumstances, making the insider stand out because no one else is exhibiting the same intensity of emotion.

All experts endorsed the value of random audits not only as a countermeasure to catch malefactors but also as a deterrent. Expert 9 summed up the 100% consensus in noting that a rigorous system of audits and reviews should discourage all but the most brilliant and determined, but that the proper

audit regime might be cost prohibitive. Similarly, and without exception, all experts would find more reason to fear the destructive capacity of the hostile insider who plans over that of the one who erupts or acts episodically or impetuously.

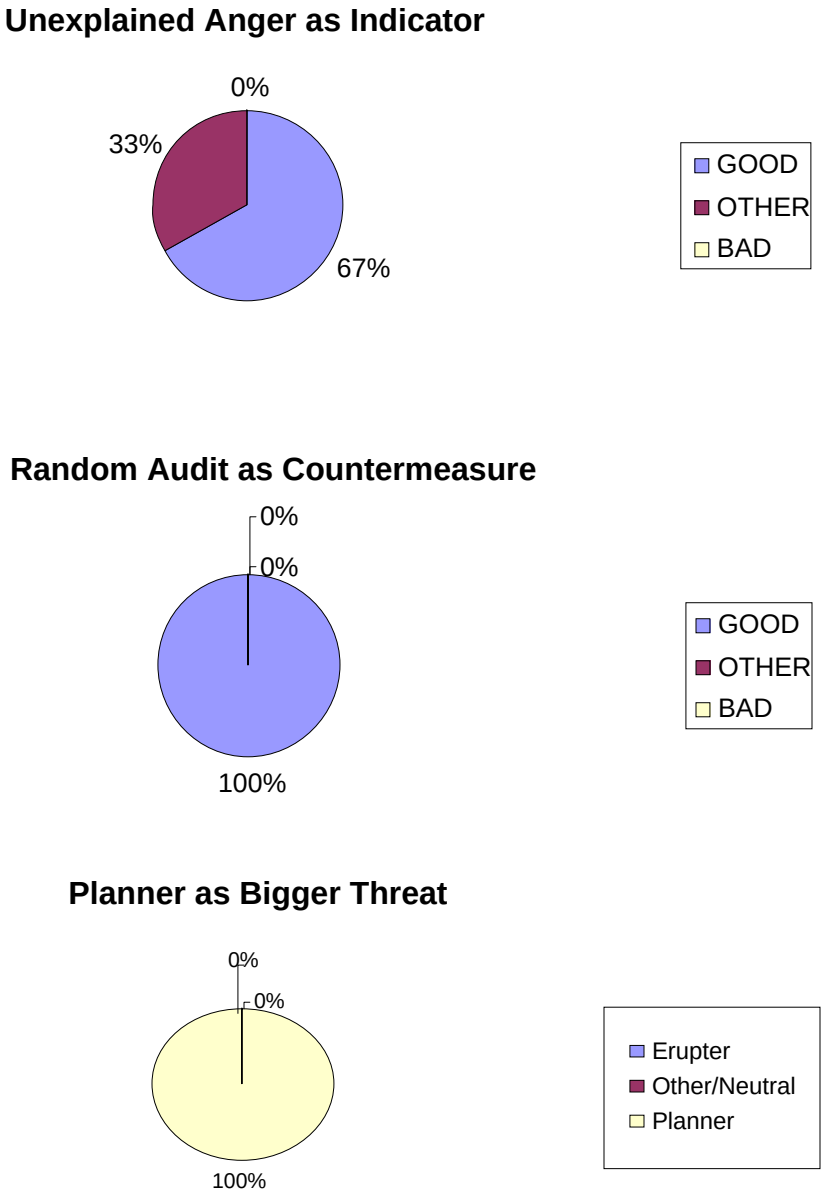


Figure 4. Areas of Convergence from Review of Delphi Round 1

Additional areas of 100% convergence were in comparative ratings of archetypal hostile insiders personified by two composite characters, a planner ("Herman") and an erupter ("Edna."). Herman represented a trust betrayer who plans an attack and generally exhibits goal-oriented behaviors, while Edna represented an individual who erupts and exhibits more reactive behaviors. In the expert judgments of which insider represents more of an institutional threat and which is more prone to carry out a complex fraud scheme, 100% of responders chose the planner. In each of these cases, Delphi experts judged it more likely that the planner composite character would pose the greater threat to the institution and also possess greater wherewithal to plan and carry out a fraud scheme that would damage the employer.

While experts generally rated the erupter as more likely to pose danger to people rather than to the institution as a whole, there was some variation and debate in ratings, as depicted in Figure 5.

Explanatory comments accompanying the ratings indicated a general agreement underlying the divergence once the rationale for the difference surfaced. The small percentages of experts who rated the planner as potentially more dangerous in a workplace violence scenario (8%), or as posing a greater threat to people in general (25%), indicated that if the planner were disposed to carry out an attack, the experts would expect this attack to be much more lethal and potentially devastating than a similar effort by a less methodical, more impulsive counterpart. Thus, in their view, while the erupter would be more prone to lose control and strike, this hostile insider's destructive impact would tend to be limited to settling personal scores more than to bringing an institution to its knees. However, if the planner were intent on carrying out an attack, his calculation would magnify the number of casualties and destructive impact.

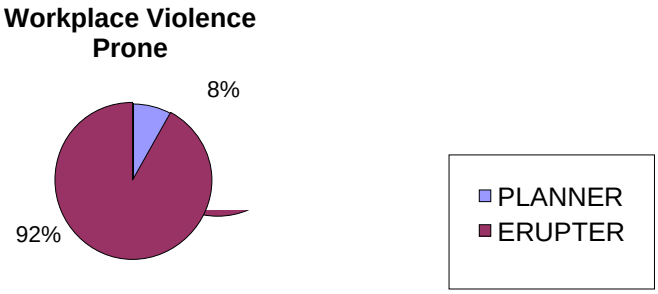


Figure 5. Variation in Expert Ratings of Planner vs. Erupter Insider Types

Interestingly, the same breakdown for People Threat in Figure 5 appeared in judgments on likelihood of this personality getting involved with an activist group with hostile intentions for the organization, shown in Figure 6.

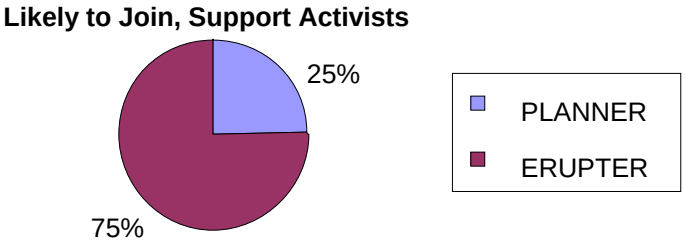


Figure 6. Planner Less Likely to Join Activists

Amplifying remarks indicated that the erupter would be more likely to seek dissident connections by virtue of feeling more removed from society (Expert 4). The planner, on the other hand, would be reluctant to associate with outside groups because he is not a joiner (Expert 1) and does not trust others readily (Expert 4). The erupter would be easier to co-opt or otherwise manipulate (Expert 5). Another respondent, Expert 12, judged the erupter more vulnerable even to being used unwittingly, whereas the planner could be more susceptible to manipulation if an activist group were to play to his ego and magnify his perceived importance to their cause.

Finally, the greatest divergence concerned which type would be more likely to compromise insider information that could serve in an adversary's targeting of an institution or infrastructure. Respondents judged the erupter more likely to compromise such information by a 2:1 margin, as Figure 7 shows. The divergence of views traced to expert opinions that the planner, might be somewhat likely to compromise information while still minimizing personal exposure to discovery, while the other, more volatile personality, would be generally more likely to compromise information with less forethought and with less regard for consequences once committed to a course of action.

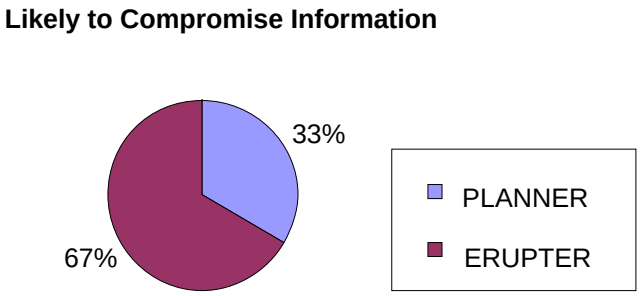


Figure 7. Compromise of Information More Likely by Volatile Insider

C. DELPHI ROUND 3: THINKING LIKE A PREDATOR

Delphi Round 3 played back the results of Round 2 to the experts in an effort to solicit validation while also preparing them to shift gears. Now, the experts had to set aside their traditional roles in infrastructure and institutional defense in order to think like an adversary and consider how they would use an insider to carry out a terrorist attack against a Level 1 infrastructure: water, power, or telecommunications.[7] Accordingly, respondents received Appendix C to summarize the findings of the preceding round, along with the questions in

[7] Recall from the questions for Delphi Round 3, Level 1 critical infrastructures, such as water, power, and telecommunications/information technology are rated as primary because of their capacity for influencing cascading failures among the rest of the critical infrastructures (Lewis, 2006, pp. 56–57).

Figure 3. Respondents also received a separate attachment, which supplied the charts and diagrams from Delphi Round 2, Section B above, for respondents interested in greater detail. Since this material is discussed at greater length in the previous chapter, it is not repeated in an appendix.

1. Overall Results of Round 3

Some themes invited strong expert convergence:

- Predominant selection of power as the best infrastructure to target, for reasons of accessibility and impact.
- Majority, two-to-one preference of experts for an insider attack relying on using an infiltrator rather than on recruiting a disaffected insider who is already in place.
- Identification of technological monitoring and No Dark Corners (explained below) work design as the more likely barriers to a successful attack, particularly when used in tandem, than such measures as random audits and background investigations, despite higher ratings for such measures during earlier Delphi surveys.
- Assessment of strong deterrent value for sting or dangle operations, which involve flushing out hostile insiders by pretext and could include luring a hostile insider to join what purports to be a terrorist organization that does not really exist or having a trusted insider exhibit behaviors that give the appearance of being an excellent recruitment target to cultivate.

Other themes that showed early promise from the same experts regarding the insider threat as defenders failed to win strong or consistent support in the eyes of the Delphi experts approaching an infrastructure target as attackers. (These apparent contradictions warrant analysis and are discussed at greater length below and in the next chapter.) Some of these:

- Brother’s Keeper option, a shorthand for security awareness programs and encouragement of co-workers to identify and act on suspicions of hostile or inexplicable insider activities.
- Random audits, which could be operational process audits, financial audits, or any combination that could potentially uncover evidence of hostile activity.
- Background investigations or updates, which involve screening of new hires and possible periodic update investigations of existing employees

2. Depictions of Findings

As for the preceding round, the results of Delphi Round 3 lent themselves to capture via spreadsheet or chart, hence, these at-a-glance summaries:

Table 5. Countermeasure Ratings by Experts as Attackers

	1-No obstacle	2-Easily overcome	3-Surmountable problem	4-Signif but surmountable	5-Potentially insurmountable
A. Brother's Keeper	0	42%	50%	8%	0
B. No Dark Corners	0	25%	25%	42%	8%
C. Random Audits	8%	42%	25%	25%	0
D. Tech Monitoring	8%	0	50%	17%	25%
E. Backgnd Invs or Updates	8%	42%	42%	8%	0
F. Sting or Dangle Ops	0	50%	8%	25%	17%

Over 40% rate as significant at some level, some potentially insurmountable

At least 75% rate as minor obstacle, handled with average resources

In Table 5, the three countermeasures that rated as significant enough to be potentially insurmountable are highlighted in yellow. Over 40% of experts saw these countermeasures, or countermeasures, representing an obstacle to attack at some level of significance sufficient to require considerable effort and resources, if not insurmountable, which represent the combined ratings of columns 4 and 5.

TECHNOLOGY-BASED MONITORING. This measure received the highest of the potentially insurmountable ratings, 25%. Yet, it also received an 8% rating of no obstacle at all. Amplifying comment from Expert 4 explained this wide range of ratings by pointing out that this kind of monitoring is not widely available or deployed across the targeted infrastructures, and in any case, is unreliably tracked and interpreted in time for targets to make effective use of it in preventing many attacks.

STINGS. Similarly, sting or dangle operations, which rated the same combined score of 43% in the last two columns, albeit in inverse proportions, also had high ratings (58%) suggesting such measures could be overcome without undue strain. Expert remarks shedding light on reasons for this variation included Expert 2's observation that a sting operation would be the greatest deterrent to recruiting an apparently disgruntled insider. However, if the trust betrayer were an infiltrator sufficiently trained in operational security, he or she would be inoculated and less susceptible to compromise than a recruit under less stringent ideological or operational control. Expert 5 noted that few critical infrastructure stewards have the stomach to support sting operations, as the negative reaction of the work force could easily result in untenable situations with the labor unions representing the bulk of the institutions employees. None of the experts dismissed this option as posing no obstacle whatsoever.

NO DARK CORNERS. Finally, this option, at 50%, represented the highest-scoring countermeasure in the combined columns 4 and 5. Experts were presented with this term as a shorthand for an array of defenses centering on a strategy that configures the job to reduce chances for a sole individual occupying a sensitive area undetected; another trusted employee must be within line of sight or some form of remote surveillance or detection must create the possibility that someone may be watching. Some of the experts had experienced this approach in the defense or nuclear security industry in the form of two-person integrity rules or no-alone zones, respectively. Here experts also diverged, with 50% rating this option just as easily yielding to average resources or easily overcome (combining columns 2 and 3). However, none of these experts dismissed this option as posing no obstacle. Expert 5 noted that this approach, in combination with technology-based monitoring, would be even more insurmountable, while Expert 7 saw this option as more effective than most human mechanisms. Expert 1 attested to the effectiveness of No Dark Corners, where feasible, but found that the nature of the kinds of target he would attack was such that minimal staffing with skeleton crews made the approach

impractical, unless supplemented with surveillance cameras or other technology that would permit real-time audit trails serving as a virtual co-pilot keeping the potential trust betrayer in check.

RANDOM AUDITS. Why would a measure universally heralded as an effective counter to insider attack in Delphi Round 2 emerge in this round as a minor obstacle in the eyes of 75% of the experts simulating an adversary? The numbers do not tell the story. The narrative remarks offer a deeper understanding of the apparently discrepant findings. Expert 2, as one who has performed operational audits to uncover foul play in a number of Fortune 100 corporations, noted that random audits are seldom truly random. Instead, an astute observer sees them coming. Moreover, audits performed by external accounting agencies tend to be relatively benign and even susceptible to organizational pressures that make a satisfactory audit the default. Even when an audit probes to the point of uncovering questionable activities, it is generally easy to bluff one's way through it. Experts who themselves regularly conduct audits to uncover fraud noted that, as much as they endorse random audits, their value is highly variable and the audits are seldom a threat of actual exposure, given sufficient preparation and maneuvering skill on the part of the person audited.

BACKGROUND INVESTIGATIONS. Several experts at one time made their living performing or managing background investigations for national defense security clearances or as part of corporate due diligence in the context of mergers or other business activities requiring verification of individual trustworthiness. Citing a current, professional reference manual, one of these experts noted that the pre-employment screening industry is relatively new, that concerns for privacy and data protection sharply limit the reach and scope of the average background investigation, and that the requirements of the Fair Credit Reporting Act generally mandate that employers disclose negative findings to applicants and allow them to correct false or misreported information (*Protection of Assets Manual*, 2006, pp. 1–IV–1 to 1–IV–18). For these reasons, the experts

schooled in this area rated these investigations as low hurdles and commented that the uninitiated tend to expect more revealing and deterrent value from background investigations than these will actually yield for targeted infrastructures and institutions. Expert 9 enlarged on this theme as follows:

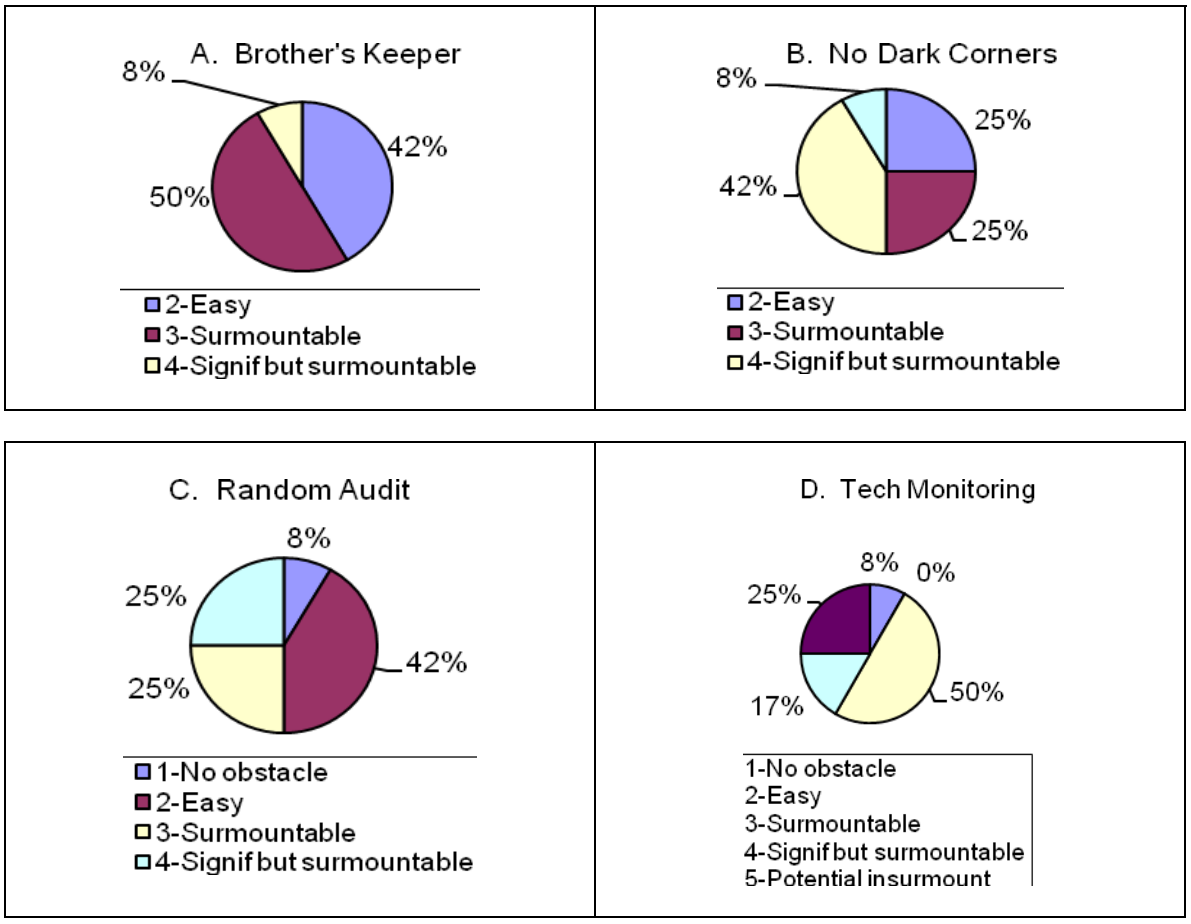
- The vetting process may be nonexistent, particularly for vendors. Yet the infrastructure site where the vendors arrive will often grant access on the assurances of the vendor firm that it has performed standard background investigations.
- When present, the vetting process may nevertheless be delayed in its execution and completion. In other words, even when vendors are operating under the assumption that their background investigation program is functioning properly, the reality is likely to be that only cursory attention has been paid to the process, with omissions in employment history left unexamined.
- The typical background investigation has multiple blind spots to disappear into. Time and budget constraints often compel the best investigator to cut corners or accept information by telephone that might raise suspicions if obtained in a field visit. Thus, accommodation addresses and false front "former employers" may be accepted as references over the telephone, when a field visit would reveal the "business" is a residential mail drop. Moreover, even the best investigative reports tend to require some arcane knowledge for proper interpretation. The clerk charged with processing this report, however, is unlikely to notice that the investigation did not cover a county of residence that was different from a county of employment claimed by an applicant—possibly because the same clerk neglected to order an investigation for the additional county, in an effort to spare time and expense. Nor will the investigation itself necessarily uncover that an

applicant has been serially rejected by other employers, since privacy concerns may well shield what would qualify as suspicious activity worthy of further scrutiny.

Similarly, Expert 11 pointed out that many critical infrastructure organizations do not perform thorough background investigations on employees or contractors, particularly if they are small or resource-constrained. Contrary to traditional reliance on the "exceptionally thorough vet" championed by counterintelligence experts (Wright, 1987, p. 301), the expert affirmed that this level of investigation is simply not an option for most infrastructure workers. Expert 4 actually selected a rural critical infrastructure target, examined its structure and operations, and determined that its management did not perform background investigations at all. Expert 7, from a national security perspective, noted that a well-developed false front and attention to maintaining a simple cover story without drawing attention are all it takes for a trust betrayer to sidestep the background investigation or periodic update. As a historical example, he cited the case of the surgeon general to George Washington, Dr. Benjamin Church. Church had unexplained, sudden wealth that permitted him to afford to keep a mistress. While Washington had excellent intelligence networks, he lacked a counterintelligence officer whose business would have been to question whether the sudden wealth-signaled agent payments from British masters or some other indiscretion might disqualify Dr. Church from a position of trust.

Experts generally noted that background investigations do deter convicted criminals and blatant malefactors. However, they also questioned their value as a countermeasure because the foregoing variation and inconsistency in background investigations neither assures nor reliably results in the desired benefit. Since the Fair Credit Reporting Act requires considerable disclosure to individuals investigated, two experts noted, a committed infiltrator can easily discern the gaps in pre-employment screening by reading such laws and performing online research. Experts also indicated that an intelligent adversary

could easily send the same applicant to multiple infrastructure employers in a given area until hired. Expert 5, for example, pointed out that aging work forces and relative lackluster appeal of critical infrastructure are such that basic skills are in high demand. Thus, anyone showing technical aptitude and an interest in accepting entry-level wages could easily find the candidate employer receptive to cutting corners to fill vacancies. Experts 4 and 11 thought that small utilities in particular were subject to relying on visceral judgments in hiring decisions. Such environments give more weight to an introduction from someone in hiring manager's community or service club than to an elaborate cover story calculated to deflect the routine probe of a consumer-reporting agency calling to verify credentials and identity. Figure 8 depicts these ratings.



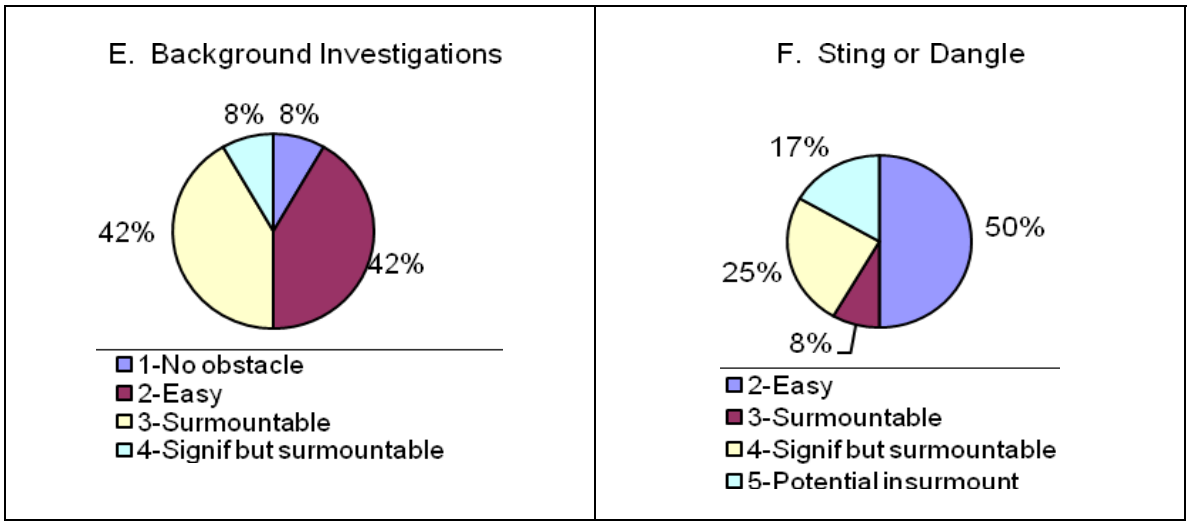


Figure 8. Expert Rating of Countermeasures Against Infrastructure Attack

Finally, Figure 9 shows strong expert convergence on both target selection and choice of insider to support an attack.

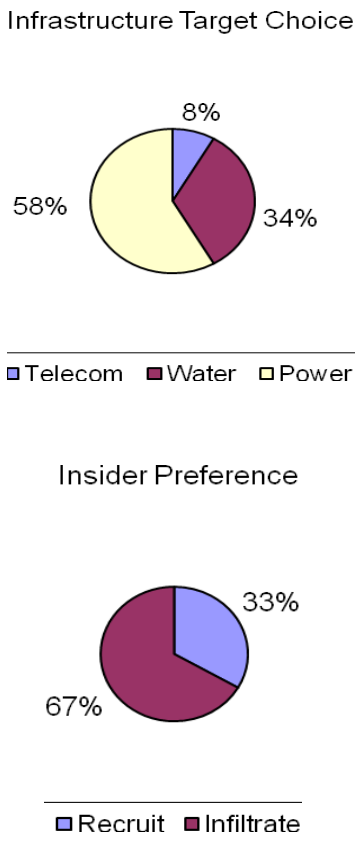


Figure 9. Target Selection and Choice of Insider for Infrastructure Attack

Experts who chose power as their target of preference, 58%, noted that, unlike water, electricity does not have reservoirs of additional supply to offset catastrophic outages and that the impact of power disruptions is more immediate and visible than similar disruptions of other infrastructures. Moreover, the opportunity for cascading failures is considerable, as telecommunications, water treatment and distribution need power to operate. Additionally, as Expert 5 pointed out, the electrical industry is in desperate need of skilled workers, and qualified individuals with skills that are in demand would likely find little difficulty in gaining employment and sufficient access to be able to discern major system vulnerabilities in fairly short order.

Similarly, water systems operated by small municipalities or remote jurisdictions would be relatively easy to penetrate and could have many of the details of their system readily available in the public domain, per Expert 11, who spent a career in this infrastructure, as well as by Expert 4, who examined one such target and found it easy to attack. Thus, 34% of the experts chose water as a viable infrastructure target

Finally, although few (8%) chose telecommunications as a target, Expert 9 approached the attack scenario by allowing access to guide target selection. He then found that telecommunications companies rely heavily on vendors, which he judged an Achilles heel and a pathway for infiltrating an agent with little risk of detection in time to prevent an attack. Specifically, Expert 9 judged private telecommunications utilities the most susceptible to vendor infiltration, especially as fiber optics facilities lease out segments of their premises to a variety of fly-by-night providers at Internet hotels. Here, each provider typically relies on unvetted legions of technical contractors of a near-infinite variety of national origins who appear at all hours of the night demanding immediate access to the facility in barely intelligible English in order to work on their client's latest communications crisis. While the majority of these individuals are no doubt technicians who are what they claim to be, a malicious new hire could enter their ranks and gain instantaneous freedom of maneuver without drawing attention.

INFILTRATING VS. RECRUITING. As Figure 9 shows, experts judged it preferable by a 2:1 ratio to infiltrate an agent rather than recruit one already in place. Experts gave the rationale for this selection as generally hinging on one or more of these factors:

Time. Given the scenario in the Delphi Round 3, questions that cited Al Qaeda-style tactics and a willingness to spend months to years before executing an attack, there was time enough to train an operative and have him or her apply to enough potential targets until hired. Then there was time to obtain system vulnerability information and exploit it before being discovered or interdicted. Because of privacy concerns, the Fair Credit Reporting Act, and lack of any mechanism within the target to track or notice an infiltrator's activities outside of the scope of employment, background investigations would offer little value in detecting anomalies. Thus, once hired, an infiltrator could make annual trips to overseas terrorist training camps, safe in the knowledge that his employer and target was prohibited from prying into his personal affairs without incurring exposure to union grievances and charges of invasion of privacy.

Trustworthiness. An infiltrator would be selected for ideological compatibility and skills suited to the attack contemplated. This individual could be expected to be highly receptive to orders. A disgruntled insider with grievances against the target, however, would likely be much more difficult to control. Lacking the same training, discipline, or motivation, recruited assets would also be more likely to compromise the attack by giving themselves away or revealing identities of co-conspirators or details of the operation.

Level of Access. Unlike access to classified intelligence information, critical infrastructure details are generally masked more by virtue of being esoteric than safeguarded. Thus, the essential information needed for targeting an infrastructure component is equally accessible to an insider who is a relative newcomer with junior-level access as to a long-term employee who possesses more arcane knowledge. The latter may have an axe to grind and a level of

emotional instability that more than offset the limited-targeting information available to an infiltrator who can be trusted not to compromise the attack.

D. ADDITIONAL EXPERT INSIGHTS AND NARRATIVES

Delphi respondents appended numerous comments with their input. Some contradicted their earlier views. For example, among the strongest initial proponents for random audits as an effective countermeasure, Experts 2, 3, and 6 later rated this measure as a marginal hurdle, if they themselves were planning an infrastructure attack. The reasoning behind this apparent discrepancy, however, became clear on reviewing their comments on conditions under which audits could be counterproductive. A sampling of indicative remarks such as these appears in Appendix D as an aid to the analysis that follows in Chapter V. In the interest of restricting the sheer volume of these remarks to manageable lengths while also maintaining respondent confidentiality, Appendix C omits reference to earthy comments and case descriptions that would likely point to the identities of some experts.

E. SUMMARY

Delphi Round 1 launched the exploration into the insider threat by canvassing the views of experts from different fields and experiences. Delphi Round 2 sharpened the focus on hostile insiders by drawing distinctions and facilitating expert convergence on indicators to monitor unexplained changes, anti-social behavior, and excessively proprietary interest in the job. Round 2 also validated expert confidence in random audits as a means of defeating trust betrayers. Round 3, however, eroded this confidence in random audits once respondents shifted gears to think like adversaries instead of defenders. They rated a number of countermeasures in terms of how much of a hurdle these countermeasures would pose in carrying out a successful attack against critical infrastructure. Experts now reconsidered random audits, previously judged as strong measures, but now diagnosed as flawed. Instead, redesign of work in a No Dark Corners approach emerged as a strong countermeasure, particularly if

used in combination with technology-based monitoring. Background investigations and periodic updates offered disappointing value as countermeasures in the eyes of the respondents who, again, noted flaws that greatly reduced their usefulness in preventing attacks or uncovering trust betrayers. Finally, Round 3 highlighted the power sector as a preferred critical infrastructure target and the infiltrator as the insider threat that experts preferred to recruiting an agent already holding access sufficient to carry out or support an insider attack.

Next, Chapter III will examine the Delphi results by establishing how the findings relate to emerging trends in an overall structure and how they inform judgments on strategies that critical infrastructure defenders can use to prevent terrorist attacks by trust betrayers.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DISCUSSION AND RECOMMENDATIONS

As the preceding chapter revealed, Delphi experts began with observations in general alignment with a model of the insider threat consistent with the existing literature. The hostile insider seemed likely to emerge as a disgruntled employee with the capacity to plan a devastating attack and the arcane knowledge to make the most of it. Indicators of this trust betrayer included unexplained anger and other suspicious behaviors, like undue secrecy and self-aggrandizement, potentially serving as red flags. Finally, countermeasures such as random audits, monitoring of employees, and investigations appeared likely to offer value as ways to thwart this kind of insider. By the end of the Delphi process, however, the same experts arrived at different conclusions. Their judgments flew in the face of this accepted wisdom.

Taken in isolation, the individual Delphi inquiries would have presented only a fragmented view instead of the more intricate mosaic that represents the insider threat to critical infrastructure. By itself, Delphi Round 1 might have stopped at a common definition of the insider threat and the realization that discovery was often retrospective, with indicators such as unexplained anger susceptible to being masked until after an attack occurred. Similarly, Delphi Round 2 might have stopped at distinguishing the main threat as a schemer who plans rather than a volatile career employee who erupts. Finally, without the context of preceding rounds, Round 3 would have probably missed concluding that the infiltrator makes the more plausible insider threat. Nor would Round 3 alone have prepared Delphi experts to delve beneath the surface to discern exploitable weaknesses of defenses such as background investigations and random audits.

Without going through the entire Delphi process, where every level of understanding was iterative, the experts would have focused too intently on the trees of countermeasures to see the larger forest of workplace realities. Thus, there would have been little opportunity to identify a systemic vulnerability in the

way targeted institutional employers limit security roles to corporate sentinels to the point of creating or ignoring dark corners where an insider threat can strike. Absent the entire series of Delphi explorations, it would not have become apparent that layering security measure atop security measure ultimately undermines trust and supplies the hostile insider more maneuvering room. Instead, the Delphi research demonstrated that a counterintuitive approach of distributing responsibility for defense among work team members and configuring work to maximize visibility to the team could provide the No Dark Corners approach discussed below.

A. WHY INFILTRATOR VS. DISGRUNTLED INSIDER?

First, research results suggested that the terrorist attacker targeting critical infrastructure would more likely use an infiltrator than a disgruntled insider already in place. A career employee with long-term access and in-depth knowledge of the inner workings of any institution or critical infrastructure will necessarily know more about how to dismantle the organization or its critical assets than an infiltrator new to the entity. The same careerist, given the time and inclination to plan, is in the best position to develop and carry out a devastating attack that circumvents defenses. However, the disgruntled insider is potentially unstable and difficult to control. According to the Delphi experts, this type is not a joiner and is likely to be too egocentric to accept direction well. Volatility makes this person an operational risk who may compromise details of an attack out of disagreement with the particulars or out of spite at not having been consulted for every move.

Additionally, in the age of the Internet and with critical infrastructure targets that have traditionally operated openly without the security precautions of the national security sector, utilities and their employees remain highly accessible. Their critical assets are immobile. Thus, they cannot move a system whose location or specifics have been compromised. In this context, the

targeting information necessary for mounting an infrastructure attack need not be so esoteric as to be available exclusively to a career insider with very detailed knowledge.

Instead, as the Delphi experts reasoned, an infiltrator who gets through the door, even at a relatively low level for a limited time, should be able to accumulate enough details to enable an attack without having to spend years masquerading as an innocuous employee. We also need to remember that Level 1 critical infrastructures are desperate for talent and have aging work forces with few systemic arrangements for recruiting, training, and deploying successors. Thus, as Expert 5 noted, infrastructure employers are prone to welcome any skilled workers without criminal convictions who show an interest in accepting entry-level positions. The same employers make frequent use of contractors who soon gain unfettered access to their systems. This situation gives an infiltrator two paths of entry: as a direct employee or as a contractor. Infiltrators may even try the two approaches concurrently without fear of one rejection influencing the possibility of another. In this milieu, if the remaining defenses (described below) are also flawed, the chances for a successful attack begin to tilt more in favor of an infiltrator than a disgruntled insider. The infiltrator may not have quite so much access, but he can definitely be better controlled, focused, and more disciplined about concealing telltale indicators of an impending attack to avoid compromising the attack.

B. TRADITIONAL DEFENSES FACING INFILTRATOR THREAT

Given the foregoing circumstances, the weaknesses of traditional defenses against this insider threat appear more evident if depicted in the context of the mutual challenges of infiltrator and defender, as Figure 10 illustrates.

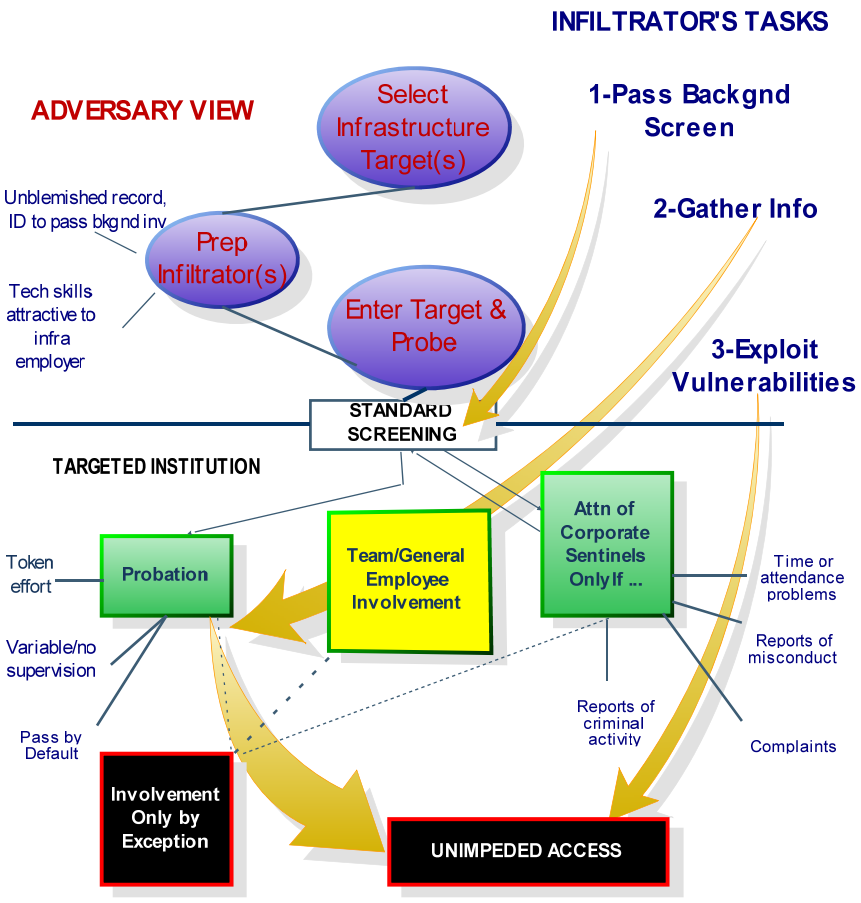


Figure 10. Traditional Situation: Infiltrator Meets Infrastructure

Figure 10 depicts the situation in which infiltrator and infrastructure find themselves when these countermeasures and their limitations impinge upon each other in the traditional scheme of penetration and defense. In this conceptualization, the adversary's job is to select a target, prepare an infiltrator, and gain entry into the target to the point of being able to probe and maneuver with unimpeded access. It falls to the infiltrator to pass the background check and then enter and pass a probationary period during which, or at least after which, the infiltrator anticipates having sufficient freedom of maneuver to gather information unimpeded by any close scrutiny or interference. The infiltrator eluding detection or interference is free to operate in the dark corners of

insufficient oversight and management by exception (*BusinessDictionary.com*, 2009), as long as his behavior and work performance do not deviate so much from the norm as to invite attention.

1. Infiltrator Step 1: Get through Screening

The standard screening, or pre-employment, background investigation presents a low hurdle to the prepared. As long as the infiltrator does not have a record of criminal convictions or obvious disqualifications, like inability to lift 25 pounds in a job whose essential functions require some manual labor, he or she has little to fear from the third party consumer-reporting agency performing the background check.

The more invasive background and update investigations permitted for national security employment are not available for the public and private sector employers who operate the nation's critical infrastructure. Nor is it feasible to demand the same level of scrutiny for a maintenance mechanic as for an intelligence analyst. Besides, the telltale component of such investigations, the probe for financial irresponsibility, is only useful in cases where trust betrayal is primarily driven by money, exemplified in the so-called "marketplace espionage" most frequently observed in counterintelligence cases of the 1980s (Allen & Polmar, pp. 3 and 47). However, as Herbig (2008, p. v) discovered in her study of trust betrayal in such cases over time, the trend in the last ten years has changed: the most common driver for today's traitors is divided loyalties, i.e., ideological rather than monetary motivation. Consequently, yesterday's focus on finances as an indicator of possible trust betrayal offers limited value in detecting today's traitors who will be living well within their means. They will also be showing no signs of the kind of debt indicative of financial hardship that would make them targets for bribery or ostensible candidates for selling out their employers to relieve financial distress Similarly, an infiltrator sent into an infrastructure employer to attack it will be unlikely to draw attention by amassing bad debts that set off financial responsibility alarms, assuming a credit report is

even requested as part of the background investigation. Nor will this individual invite negative scrutiny through drunk driving or criminal convictions that the average background investigation detects through a standard check of superior court records in counties of residence and of employment.[8] Insulating the infiltrator even more from what such background investigations uncover is that the infiltrator is already under the control and sponsorship of a primary, albeit undisclosed, employer: the attacker. Thus, the infiltrator is seeking infrastructure employment not so much for monetary or professional rewards as for access to an assigned target. Meanwhile, the attacker coaches the infiltrator to avoid actions that would raise eyebrows. Moreover, the larger and more sophisticated the attacker's organization, the more candidates available to choose from in qualifying an infiltrator, and the more likely that the ultimate selectee will arrive on the job with an unblemished record.

To complicate matters more for defenders, the legal constraints affecting employers in America severely limit a critical infrastructure steward's ability to expand the scope of a background investigation or to use its product in any way that is not demonstrably related to a given job vacancy (Equal Employment Opportunity Commission, 2009, pp. 1–6). The same applies to any program for performing update investigations on existing employees. As one industry guideline cautions, "The consideration of extraneous information that is not a valid predictor of job performance can create a source of liability" (*Pre-employment Background Screening Guideline*, 2006, p. 24). In the context of employment laws prohibiting job discrimination yet defending privacy, it is the rare hiring manager who dares flaunt such guidance by rejecting any otherwise qualified applicant, even if subtle or stated antipathies against the United States surface during the hiring process. Fidelity to America is seldom called out as a hiring criterion for work at a utility that operates critical infrastructure. In the

[8] In the United States, employment-related investigations can only legitimately use conviction records, not arrest records. Only law enforcement has access to the latter and is prohibited from sharing them with employers so that the latter do not unfairly affect an applicant's livelihood by making adverse hiring decisions before the legal system has decided actual guilt (*Pre-employment Background Screening Guideline*, pp. 20–24).

broader context of employment law, anti-discrimination protections, and limitations on the extent to which employers may practically scrutinize applicants for work at critical infrastructure sites, background investigations are unlikely to unmask any but the most unsophisticated of infiltrators.

Update investigations, if performed at all, typically come after seven years because this is the standard limit that many states and the Federal Credit Reporting Act recognize as the maximum period for making criminal history available for retrieval for employment purposes (*Pre-employment Background Screening Guideline*, pp. 20, 22). Like pre-employment investigations, updates performed through a credit bureau or other agency falling under the rules of this Act must also be fully disclosed to the subject of the investigation. An infiltrator requiring more than seven years to gather insider information to support an infrastructure attack would have aged enough to cast doubt on his or her motivational zeal and to be suspected of beginning to identify too closely with the target.

2. Infiltrator Step 2: Gather Information

As Figure 10 shows, once safely through the door, the infiltrator now interacts primarily with fellow employees and a boss, who supplies the institution's direct oversight during the probationary period. Corporate sentinels, whether security staff, auditors, information systems guardians of the computer network, human resources recruiters, attorneys, or others with assigned responsibility for various monitoring functions rarely interact with the new employee. They may participate in a new-hire orientation, but otherwise deal with the newcomer only if the latter's actions or questions affect their various disciplines. The new employee benefits from a grace period during which minor transgressions committed in the course of gathering information are easily dismissed as a rookie's excusable faux pas. Unless the neophyte does something egregious to excite remark, he or she is unlikely to face a random audit or active monitoring of computer key strokes, or time and duration of

access into a given work space. On the rare occasion when an infiltrator's actions invite challenge, all that are necessary to deflect focused attention of corporate sentinels are a ready apology and a profession of ignorance.

To further limit opportunities for detecting an infiltrator's suspicious gathering of insider information via random audit, Delphi experts in business and operational audit note that so-called random audits are seldom truly random. As Expert 2 pointed out in the preceding chapter, the astute observer sees them coming. Moreover, many audits are perfunctory, particularly if auditors consider themselves overextended and loathe taking on the extra work of sustaining a negative finding. As one analyst found in a longitudinal study of organizations susceptible to accountability failures, cases are "resource intensive and, as a result, enforcement is necessarily selective" (Fishman, p. 274). This explains why a resource-intensive audit will not be "wasted" on a neophyte who has still not even passed probation.

In many, if not most critical infrastructure environments, audits are by definition adversarial. They are, therefore, regarded as a necessary evil perpetrated by individuals who are more tolerated than esteemed. To the extent that auditors are aloof, disdainful, or menacing, they struggle to obtain active cooperation. Expert 11 has seen that co-workers are even more likely to defend than to report a trust betrayer who has managed to come across as "just one of the guys." The greater scrutiny is likely to focus on activities affecting financial performance or high-value losses. However, until the moment of attack, the infiltrator targeting critical infrastructure is unassociated with any loss-producing events that would invite such scrutiny. In such circumstances, it is the rare audit that will identify and focus sufficient attention on an infiltrator to elicit anything more than an oral warning or mild rebuke. Consequently, the traditional audit poses no threat to the infiltrator operating with a modicum of training and sophistication.

Technology exists to remotely monitor every keystroke an employee makes whether operating a desktop computer or a supervisory control and data acquisition (SCADA) system—the principal means of controlling valves and distribution of signals, power, or water when handling a critical infrastructure component. It is possible to configure control room access so that no one individual may enter a critical area alone. It is also possible to monitor such areas remotely through video surveillance. These capabilities can theoretically prevent all but the most astute from carrying out undetected acts of mischief. However, when applied to the challenge of detecting and thwarting an infiltrator bent on attacking critical infrastructure, technology alone falls short, for several reasons. First, for every device capable of tracking activity, there must exist somewhere in the institution a means of discriminating untoward activity from acceptable routine. A surveillance camera or automated log cannot by itself tell whether an operator laying hands on a SCADA panel is doing his job or interfering with another's. Such a determination requires human judgment. True, some automated tools can approximate a level of human judgment, if given precise details and parameters of what kind or number of transactions become suspect once they exceed a certain frequency in a given time period or take up significantly more time than necessary. However, the effort needed to establish these boundaries and the resources necessary to automate associated triggers exceeds the capacity of the average, financially strapped utility. Nor is this investment in proportion to the expected benefit. The same caution applies to the labor-intensive alternative to this technology-based solution: invasive snooping by a designated monitoring force. Delphi experts with career experience as line managers in critical infrastructures opined that such snooping negatively affects productivity and morale, while often leading to an unintended consequence. It sparks the creativity of aggrieved operators to find new ways to elude or defeat monitoring systems because they dislike being watched like wayward children. Thwarting such corporate sentinels, whether human overseers or automated devices, soon becomes part game, part badge of honor.

Operators then transfer this knowledge of how to bypass what they regard as invasive monitoring to peers and newcomers alike—including the potential infiltrator—because they know that if all the workers are defeating Big Brother, then management will be unable to single out any one employee for punishment.

3. Step 3: Exploit Vulnerabilities

At this point in the penetration effort, if the infiltrator has managed to survive the screening process and stay under the radar of corporate sentinels, inertia and initiative are on his side. The more he blends, the less he stands out, and the more likely he is to gain the unwitting support of co-workers and management alike, particularly if seen to be a competent team player who gets along well with others.

One contradiction in defensive strategy highlights how traditional measures can be self-undermining. The common thread that unravels the foregoing defenses when exploited by an infiltrator or any hostile insider is a lack of active involvement on the part of the workforce on the one hand, tied with what infrastructure workers perceive as the offensiveness of too much oversight, on the other hand. One career analyst of trust betrayers explained the latter phenomenon by stating that vigilance against disloyalty “threatens the ecology of trust and raises the likelihood of disloyalty because of a motivation to resist excessive oversight “(Carney, 1994, p. 21).

In this context, the institution comes to rely excessively on its corporate sentinels, viz. its designated watchers, such as security staff, leaving the rest of the workforce indifferent to a defensive role that the employees and managers leave to such specialists. Meanwhile, the capacity of these sentinels, to focus limited resources on discovering a needle-in-the-haystack level of visibility of an insider threat is constrained by infrastructure operator resistance to draconian security measures that are too costly and impede operations. Into the space between general employee indifference and constraints on corporate sentinels, the infiltrator and any insider threat can create a dark corner to carry out hostile activity with impunity.

C. ALTERNATIVE APPROACH

One way to overcome the vulnerabilities in the foregoing defensive measures is to re-examine Figure 10's penetration sequence in light of how a different strategy might apply the same institutional resources to better effect. Figure 11 shows such an alternative end-state.

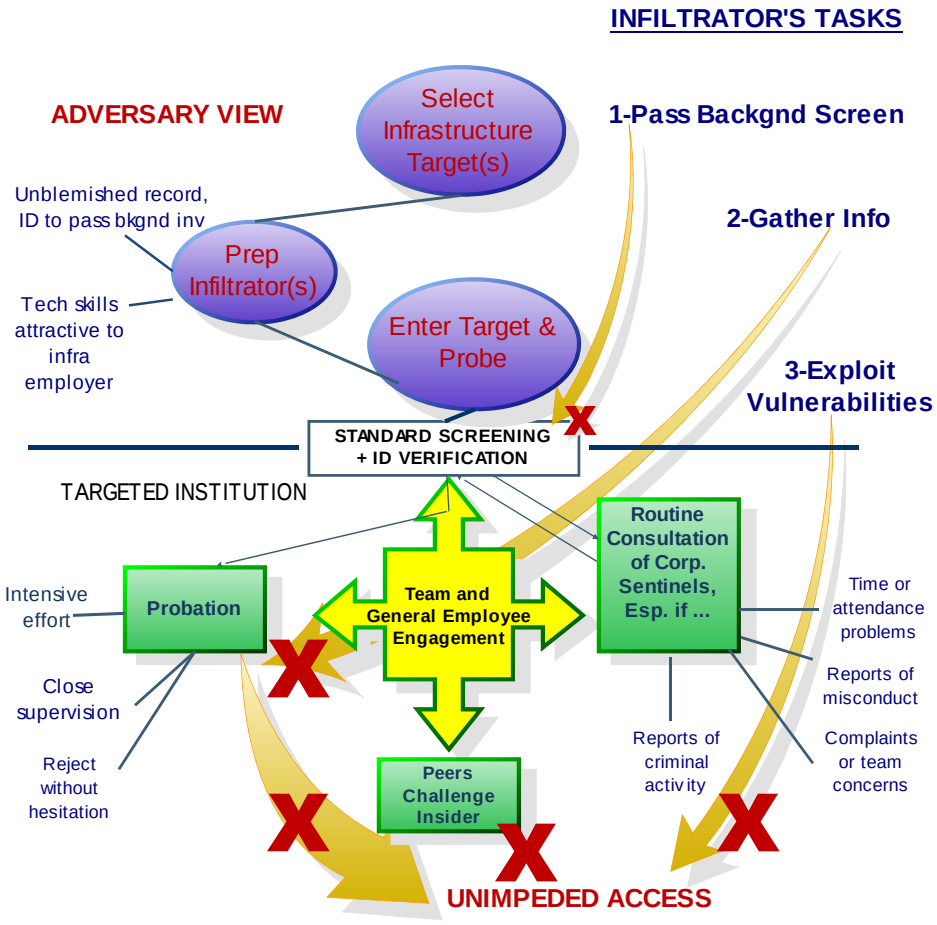


Figure 11. Desired End-State for Infrastructure vs. Hostile Insider

What has changed? First, the screening process no longer relies excessively on a search for indicators that uncover neither infiltrator nor other hostile insider. As one executive who studied trust betrayal for an entire career pointed out, many experts find that personnel investigations do not prevent espionage or detect those who may commit such a crime (Anderson, 1994, p. 7). Instead, the process now pays special attention to verifying identity. It takes

advantage of government resources through a program that U.S. Immigrations and Customs Enforcement (ICE) makes available to companies and infrastructure institutions alike—ICE Mutual Agreement for Government and Employers (ICE/IMAGE). For a fraction of the resources necessary to conduct update investigations of utility employees every seven years,[9] infrastructure employers can instead devote more attention to verifying basic identity and right-to-work authorizations of new hires in order to defend against potential infiltrators. They improve their internal capacity for such detection by availing themselves of a federally funded program that trains human resources recruiters to check credentials and gives them access to Social Security and immigration databases to facilitate verification of employment eligibility (*ICE Mutual Agreement for Government and Employers*, 2009).

The new screening program will not necessarily catch all infiltrators any more than it will defeat individuals who enter the institution benevolently and only later develop hostility and a propensity to betray or destroy. However, the program will reduce the ability of terrorist organizations to infiltrate their agents with falsified credentials, which absent increased scrutiny receive only token examination from the most junior clerk assigned to employment application processing functions. This is why Figure 11 shows a smaller X next to the arrow depicting the infiltrator's first task. The new screening program complicates the challenge for the infiltrator, but does not eliminate it altogether.

More importantly, however, the biggest change from the Figure 10 traditional approach to the Figure 11 alternative is the active engagement of the general employee population. Employees now support the screening process by at least verifying credentials through their own professional and trade networks. The immediate supervisor monitors the employee closely throughout the probationary period. During this interval, the new default expectation is not that

[9] The seven-year number is based on the standard state limit for reporting of criminal convictions and that the Fair Credit Reporting Act uses for employment-related background screening (*Pre-employment Background Screening Guideline*, pp. 20, 22).

all newcomers pass probation absent egregious incidents, but that all are released from probation unless they demonstrate talent worth keeping. This demonstration must satisfy not only the supervisor but teammates as well, which forces close interaction on a daily basis. Moreover, during probation, new hires are treated like student pilots who are not ready for solo flight—never left alone in the cockpit. Only, in the case of critical infrastructure, the student is a new employee and the cockpit is any critical asset or control system. At the same time, this alternative approach requires a culture of constant team interaction and self-monitoring that reduces opportunities for probing and undermining the institution clandestinely. It eliminates the dark corners represented by the black boxes in Figure 10 because in Figure 11 employee oversight means there are fewer places to hide. This is the No Dark Corners approach that configures the job to reduce chances for a sole individual occupying a sensitive area undetected. It breathes life into this security prescription of management expert Tom Peters when exhorting security professionals not to see their contribution exclusively in the character of corporate sentinels:

> I don't want you to be security people for the organization, but to make everyone else in the organization a security person. You don't "do" security. You help all the employees do it … You win the game when I and my colleagues are the real security people in the place. (Peters, 2007)

At the heart of the cultural shift, this alternative approach also increases the opportunity to defect any insider threat because it spreads defensive responsibility pervasively, rather than relying exclusively on corporate sentinels.

D. BALANCING TRUST AND TRANSPARENCY: THE CO-PILOT MODEL

How can a cultural shift in the workplace create a team whose members constantly monitor each other without undermining the trust necessary for internal cohesion? On the surface, it would appear that such a team is merely relieving assigned corporate sentinels of their snooping duties. After all, as organizational consultant Stephen Covey has observed, suspicion can generate

the behaviors that managers and leaders are defending against, thus fostering a collusive environment of distrust (2008, p. 292). Extending the pilot and cockpit metaphor from the preceding discussion on probation, however, offers an answer to this apparent contradiction.

In line with the cultural shift to internal team monitoring, every team member becomes not an inquisitor but a co-pilot. The key elements of the co-pilot definition that apply are of a "qualified pilot who assists or relieves the pilot but is not in command" (*Merriam-Webster*, 2009). The co-pilot has a vested interest in maintaining safe altitude and air speed and in arriving on schedule at the right destination. Applied to the work team, this model makes every team member a co-pilot. Neither a co-pilot nor a team member need become a snoop or tattletale. Yet both should be in a position to fully monitor what is happening in cockpit or control room, with aircraft gauges or with SCADA displays. In this context, a co-pilot level of engagement becomes cohesion producing because it demonstrates a shared sense of ownership in the team's work. (See Appendix D, items 1, 2, and 5 for Delphi respondent illustrations of such conditions in action.)

While many parts of a given countermeasure carry forward into the new framework, the means of applying the countermeasure changes fundamentally. No Dark Corners transforms invasive techniques into performance gauges for work teams. A video camera monitoring a critical process involving hazardous materials should now be welcome as a way for a fellow team member to be able to summon assistance if another team member in the area gets hurt—not as a spy camera for helping bosses catch subordinates in the act of violating established procedures. The same cultural shift should make team members appreciate having a back-up control room operator or lineman within earshot or line of sight rather than bristle at the thought of not being trusted to work alone. Embracing the co-pilot model should transform additional physical or electronic monitoring into a welcome means of summoning assistance. It should also limit opportunities for a hostile insider to act against the institution. Ultimately, greater

transparency and work redesign should limit opportunities for clandestine and damaging activities by eliminating the dark corners that insider threats need to do their worst.

E. CONTRAST WITH TRADITIONAL APPROACH

Applying the No Dark Corners strategy communicates to the would-be insider threat that someone may be watching. In a traditional approach, the watcher is a corporate sentinel, and there are seldom enough of these watchers to monitor every process or venue. By contrast, in a No Dark Corners arena, the one who may be watching is a co-worker who has a proprietary interest in the institution and will therefore act to defend it.

Figure 12 highlights key features of this strategy, showing innovations, as well as what management authority Peter Drucker emphasized as a primary duty of all organizations: organized abandonment of processes and strategies that are no longer working (Drucker, 2002, p. 295). A method of fostering the creation of innovative strategies according to some observers, this grid challenges the institution to act on four key features in order to arrive at meaningful innovation (Kim & Mauborgne, 2005, pp. 35–27).

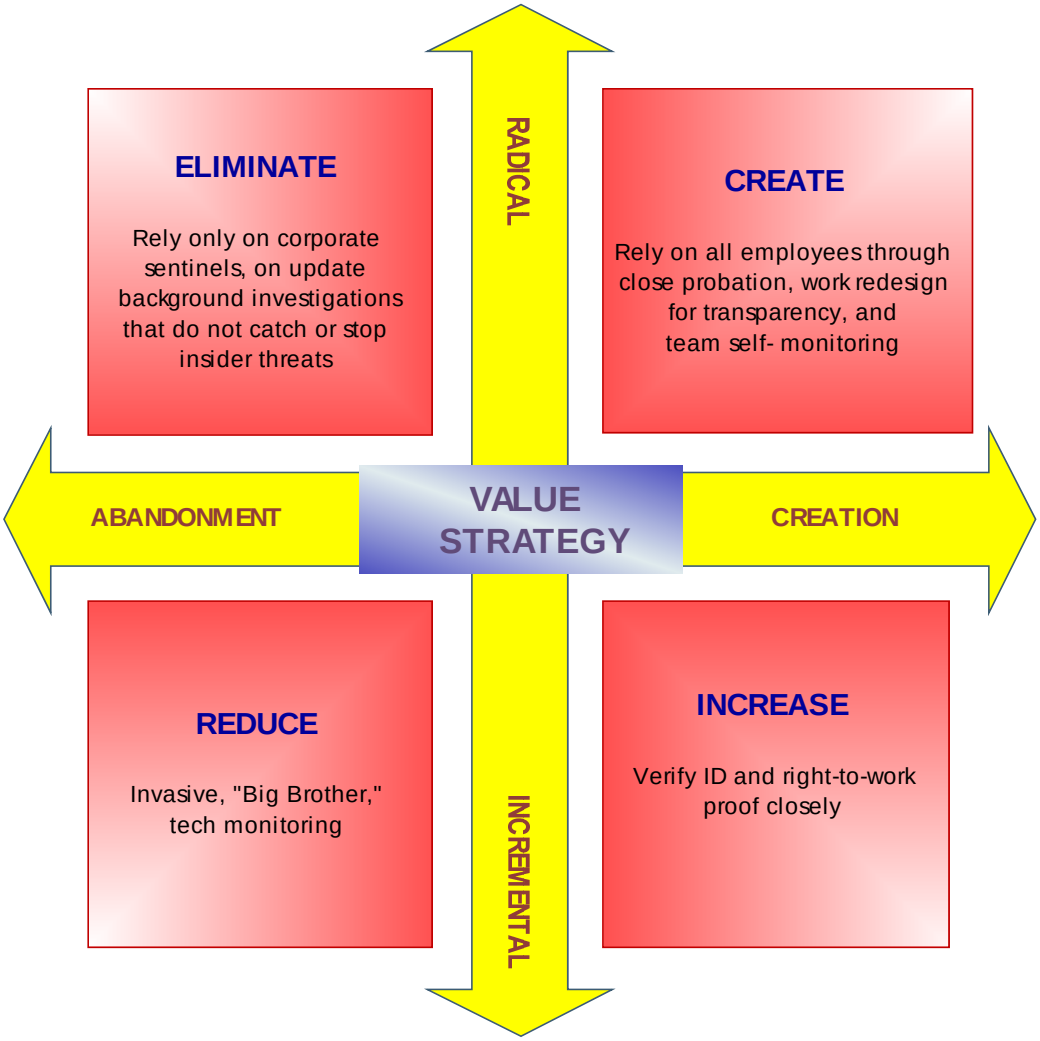


Figure 12. Key Features of No Dark Corners Strategy

As Figure 12 shows, measures that impede an infiltrator's ability to surveil or strike take precedence over measures that are easily bypassed and offer negligible value in defeating an insider threat. Organizing these measures to contrast them with the traditional defenses that accepted wisdom favors underscores even more the distinctions of the No Dark Corners approach. Figure 13 presents this contrast in the form of a strategy canvas where the status quo appears in red and a breakaway challenge to this strategy, i.e., No Dark Corners, appears in blue.

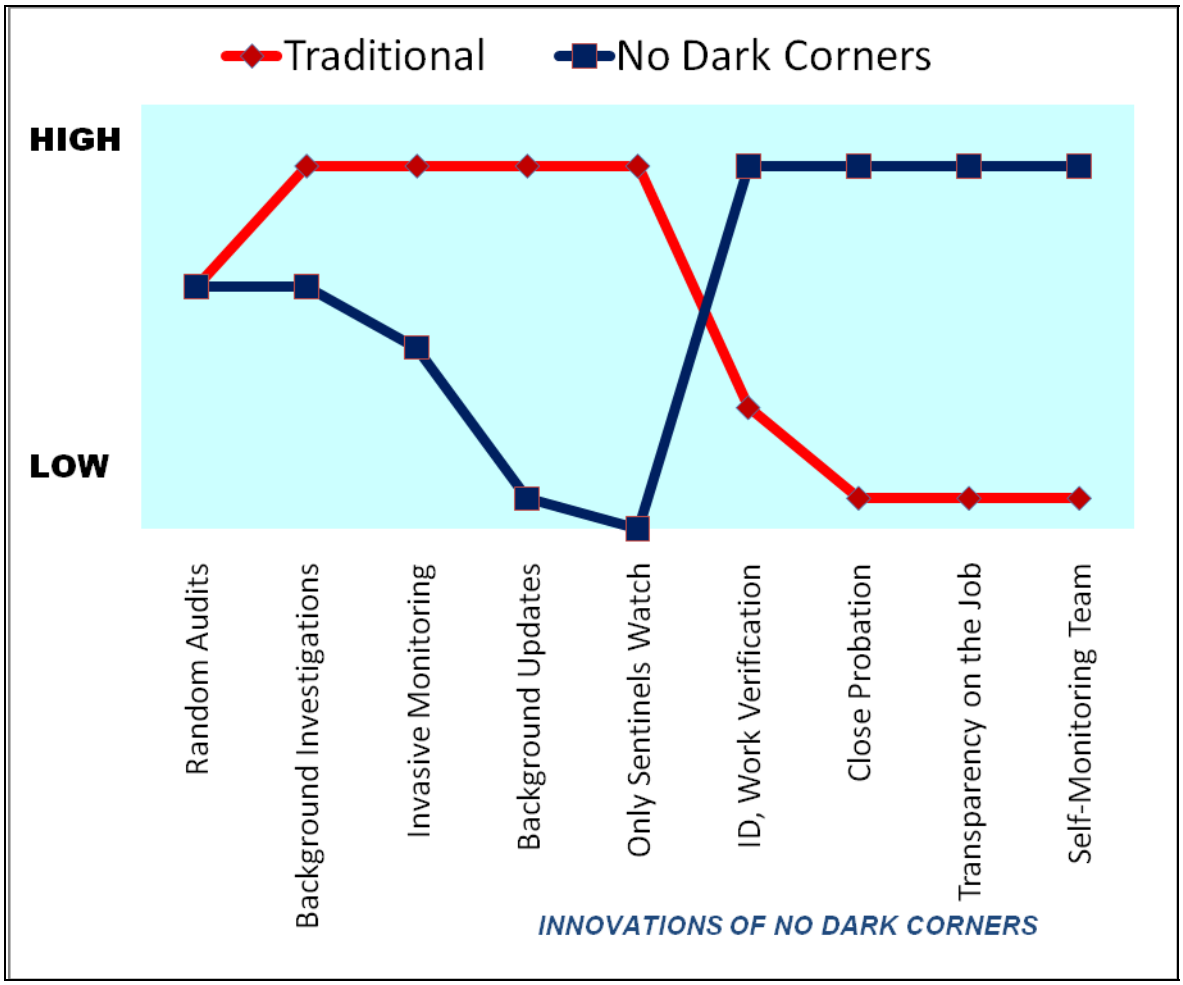


Figure 13. Strategy Canvas: Traditional vs. No Dark Corners

The strategy canvas is at once a gauge and a framework for revealing where traditional insider defenses have faltered and where the innovations of No Dark Corners offer alternatives to reduce chronic vulnerabilities. The canvas visually communicates the current state of affairs in insider threat defense (in red) while also showing the potential for breaking new ground (in blue) to reduce susceptibility to infiltrators and, by extension, to any hostile insider.

In addition to adjusting defensive measures already discussed at length throughout these pages, Figure 13 draws attention to three particular innovations that reflected insights both of Delphi experts and of published analysts of trust

betrayers. These three are close probation, transparency on the job, and team self-monitoring. All three measures offer productivity value, as well as defensive benefits.

CLOSE PROBATION. As one study shows in extolling the virtues of close probation for example, “organizations that systematically integrate new employees enjoy lower turnover, and the recruits report greater commitment and job satisfaction” (Fernandez-Araoz, Groysberg, & Nohria, 2009, p. 84). This and the other tools intend to defeat hostile insiders through the kind of scrutiny that corporate sentinels cannot match, namely, the scrutiny of a co-worker, or what one analyst calls a “citizen-sentry” (Fishman, 311).

In critical infrastructure institutions, probationary periods are the ideal means of rejecting a new hire for any reason, without having to meet the rigors of bargaining unit constraints that are the equivalent of academic protections for tenured professors. Yet, Delphi respondent experience shows that two parts of the probation process are under exploited. Hiring managers hesitate to release probationary employees, particularly if the internal hiring process is lengthy, complicated, and demanding of management time. To make matters worse, in many cases, the longer a vacancy goes unfilled, the greater the chance of losing that position, as upper management can see that work goes on despite the vacancy. Finally, in areas where supervision is traditionally lax, mentoring and monitoring of probationary employees is absent, thereby, predisposing hiring managers to keep the probationary employee by default. In reversal of this process, No Dark Corners puts a premium on using the probation period as a line of institutional and infrastructure defense. The default shifts away from keeping the new hire absent overwhelming evidence of a problem. Instead, the default becomes termination at the first sign of any problem and automatic release at the end of probation absent ostensible proof that the new employee adds value. The only way for this proof to surface is through close supervision, which means active engagement of front-line supervisors and fellow members of a work team.

The supervisor acts as the pilot, with the rest of the team members as co-pilots—all having a vested interest in assuring that anyone joining their ranks can be trusted in their institution's equivalent of the cockpit.

TRANSPARENCY ON THE JOB. In keeping with the new strategy for maximizing the value of probationary periods, transparency on the job means that every task, operation, or action performed at a critical infrastructure site should be within the actual or virtual line-of-sight of a knowledgeable peer or supervisor. Evoking the two-person-integrity rules of working in some classified environments (See Appendix D, item 2 for more details.), every job and work space should be designed to maximize visibility to peers and minimize opportunities for clandestine, hostile action. While Level 1 infrastructure utilities seldom have the staffing to implement a forced buddy system like this under all circumstances, the selective use of surveillance cameras to monitor critical operations can at least reduce infiltrator assurance that clandestine attivities will remain undetected. The deterrent value of this kind of system is analogous to that of having surveillance cameras and their associated video monitors openly placed near the cash register at retail convenience stores. This practice in retail security is thought to deter robbery because of the uncertainty it creates about who may be watching in the eyes of the potential robber (Nieto, Johnston-Dodds, & Simmons, 2002, p. 34; Murphy, p. 19, 1999).[10] Process-monitoring cameras, which assist with environmental watching of systems to be sure they are operating within design tolerances and of hazardous areas in order to dispatch rescue crews, are already commonplace at infrastructure sites, as are security surveillance cameras and access control systems in public areas, particularly in Britain (Nieto, Johnston-Dodds, & Simmons, 2002, p. 16; Day, 2009, p. 19).[11]

[10] Patrick Murphy, Loss Prevention Director for Marriott International, confirmed experiencing an 84% decline in losses from armed robberies as a result of such an openly visible installation of surveillance cameras, which led him to publish his experience as a best industry practice in 1999 (personal communication, July 23, 2009).

[11] Richard Day, a manager whose British firm had been experiencing high losses of construction equipment to burglars, credited remotely monitored surveillance cameras for reducing such losses by 80% as of June 2009.

Designing new work sites, as they come online, to increase such visibility reduces the perception of concealment opportunities and increases the opportunity for fully engaged team members and other employees to spot untoward activity while in the course of routinely looking out for each other.

TEAM SELF-MONITORING. Finally, No Dark Corners recognizes and seeks to exploit the difference between over-the-shoulder audits and self-policing out-of-work team cohesion and pride. As Expert 6 observed, the most effective use of audits occurs when internalized at the work team level. Instead of shrinking from oversight as a form of witch hunt, team members focus on "how we can make things better" discussions. By including such discussions in regular team meetings and also encouraging informal one-on-one comments between employee and supervisor after each formal meeting, members should become their own most ardent diagnosticians. This self-monitoring presents an imposing threat of discovery for the infiltrator who may be adroit in hiding from corporate sentinels but cannot hide from the team.

As Expert 11 noted, metrics by themselves may supply only an illusion that management can track all work and make necessary course corrections in time. As a senior executive in a large infrastructure organization, he found that he did not have time to read let alone check for discrepancies in employee performance based on all the timekeeping, output measures, budget variance, and failure analysis records available only to senior executives. So, Expert 11 pushed out these data to front-line managers who could at least track themselves and their own team. As a result, the managers and soon the team members started gauging themselves and monitoring their own performance, improving effectiveness in the process. Some teams competed with each other in friendly rivalry. More teams and their managers, though, began competing with themselves, striving to beat last month's or last year's best record. Expert 11 reasoned that this kind of self-monitoring, properly encouraged and applied to defense against insider threats, would present an almost insurmountable obstacle to infiltrators intent on an attack against critical infrastructure.

F. NO DARK CORNERS' LINKAGE TO OTHER SECURITY STRATEGIES

The No Dark Corners strategy of configuring work space for maximizing opportunities for teammates to exercise a proprietary interest in their work and for promoting transparency relies on employees—legitimate insiders—defending an institution and its infrastructure by taking ownership. No Dark Corners is to critical infrastructure what Defensible Space is to community housing and Fixing Broken Windows is to community policing: a defensive strategy relying on legitimate users of a given space or activity to exercise a proprietary interest sufficient to defeat adversary encroachment. In his seminal work, architect Oscar Newman (1972) examined data from housing projects in New York to make a case for reconfiguring residential areas to enhance the natural human tendency of territoriality. In his words, "defensible space is a model for residential environments which inhibits crime by creating the physical expression of a social fabric that defends itself" (Newman, 1972, p. 3).

While Newman made efforts to extend his work to nonresidential environments with government sponsorship, the latter appeared to make little progress in the course of 20 years, despite considerable investment (O. Newman, personal communication, November 21, 2002).

In a variation of Defensible Space applied to order maintenance in public spaces, James Q. Wilson and George Kelling offered Broken Windows theory ten years later (Wilson & Kelling, 1982). Then Kelling's follow-up research demonstrated multiple successes in crime reduction in major urban cities (Kelling & Coles, 1996)—all based on the premise that neighborhoods decay into crime and disorder if the little things, like broken windows, remain untended (Kelling & Coles, p. vx). Soon, vandals break all the remaining windows. Conversely, attention to the little things, like fixing broken windows, sends a communal

message of a sense of ownership. This demonstration of proprietary interest, in turn, deters offenders, driving them away from defended areas.[12]

No Dark Corners extends the foregoing theme of a sense of ownership to critical infrastructure, in a way that recalls the housing application of *Defensible Space* and the community order maintenance of *Fixing Broken Windows*. The difference is that while the other two models apply exclusively to public spaces, No Dark Corners adds private space into the mix, however, as all critical infrastructures have control rooms and physical assets that are not open to the public, hence, out of the public view. Invariably, however, critical infrastructures also include important assets that are exposed to public view, such as transmission lines and aqueducts, which may be visible or accessible by members of the public.

Why has this not happened before?[13] First, infrastructure defense is assumed to fall primarily into the hands of the private sector, which operates 85% of critical infrastructure (Lewis, p. 56–57). By extension, the critical assets must, therefore, be under private control, hence, not in the kinds of public spaces where there apply existing models of defense through a sense of ownership, like Defensible Space and Broken Windows theories. The reality, however, is that

[12] Kelling's theory is not without its critics. However, much of the criticism is directed not at whether Fixing Broken Windows works to take back public spaces from offenders who otherwise scare legitimate users of the public away, but at larger societal issues, such as the inevitable displacement of offender activity that occurs in neighboring communities that are not using the same strategy. The criticism is along the lines that applying Broken Windows just pushes a problem from one neighborhood to another. Similarly, other critics object that changing demographics may also account for crime, thus bringing into question Broken Windows as a panacea. One criticism even went so far as to opine that greater access of unwed mothers to abortion should account for crime reduction because children who would have grown to be criminals were aborted, and Kelling did not credit this phenomenon in his theory (Levitt & Dubner, 2005). Since Kelling did not offer his theory as a panacea or as the sole explanation for decreases in crime, himself taking account of other factors, including Newman's work, it is more accurate to say his theory may have been challenged but not discredited in terms of actual aims and results. More recent criticisms focus on community policing aspects of the theory, which vary greatly depending on the police force. However, researchers, Braga and Bond, highlighted this point but vindicated the theory in a recent study, which found that cleaning up the physical environment in Lowell, MA, was very effective, while a corresponding increase in misdemeanor arrests was not (Johnson, 2009).

[13] Item 5, Appendix D, offers one Delphi expert's perspective on this topic.

critical infrastructure may be impossible to secure in some cases, as in transmission lines, aqueducts, and fiber-optic cables stretching across broad expanses of undefended territory.

No Dark Corners reduces relatively unproductive but resource-intensive investment in countermeasures that an infiltrator can readily bypass. The strategy shifts exclusive reliance of institutions on overly specialized monitors, the corporate sentinels, to the larger employee population, especially the work team closest to the infiltrator or other hostile insider. It also redirects some investment away from moderately useful pre-employment background investigations and unproductive update investigations, which may deter obvious criminals but will not defeat a hostile infiltrator.[14] Instead, the strategy shifts this investigative scrutiny to verifying identity and right-to-work documentation, which takes the form of supplemental identification, and which the Immigrations and Customs Enforcement arm of DHS is advancing through its ICE/IMAGE program of enhancing the capacity of all employers, including infrastructure stewards, to close the door to a major penetration vulnerability in the hiring process (op cit).

At the same time, this new strategy brings to bear the tools of close probation, work redesign for transparency, and self-monitoring for greater engagement of the employee population and, in particular, the work team.

G. ENVISIONING A NO DARK CORNERS WORKPLACE

In a No Dark Corners workplace, standard screening will have new emphasis on identity and right-to-work verification and false credentials will be subject to discovery, making it particularly difficult for a foreign adversary to penetrate an American institution. Close probation means an infiltrator will face unabated scrutiny, supervision, and evaluation. Similarly, a fully engaged

[14] Basic pre-employment background investigations continue to offer value as a tool of due diligence that may detect or deter criminals and individuals with a history of misconduct. They do not pose a seriously to a moderately prepared infiltrator whose selection will in some measure depend on having a history free of criminal convictions and otherwise free of easily identifiable discrepancies that background checks are designed to spot.

employee population and work flow design that eliminates hiding places while promoting transparency will reduce opportunities for the infiltrator gathering sensitive information unrelated to the individual job and breaching protocols under the banners of ignorance or deficient supervision. Corporate sentinels previously mistrusted will be accessible to team members to follow up on their concerns and suspicions. In the process, the sentinels themselves will become part of the extended family seen as supporting the work team. Opportunities for unfettered, clandestine access will be severely constrained, subject to monitoring by people or devices, and too limited to exploit reliably.

H. LIMITATIONS AND OPPORTUNITIES FOR FURTHER RESEARCH

Just as Kelling's 1996 work on Broken Windows took experimental efforts in several municipalities to support the theory he and James Q. Wilson first espoused in 1982, No Dark Corners awaits the refinement and validation that would follow introduction of this model into an institution that acts as a critical infrastructure steward. Ideally, such an institution could be compared to a sister utility or agency of comparable size and function. Results of this comparison would draw on a broad array of metrics, including measures of general productivity, positive or negative impacts attributed to insiders, and relative expenditure of resources for defense against adversaries. Alternatively, a single institution adopting the No Dark Corners strategy could compare itself across a similar scale to determine the impact of the new strategy in relation to previous experiences with insider problems under alternative defensive strategies.

I. CONCLUSION

As this study suggests, a hostile insider needs three essentials to carry out an attack against critical infrastructure: a worthy target, an open door, and a dark corner. Any adversary seeking to strike a devastating blow against any institution needs the same.

Level 1 critical infrastructures, such as power, water, and telecommunications make worthy targets. Not only are some of them irreplaceable, their damage or destruction leads to cascading failure of other, interdependent infrastructure components, from banking and finance to emergency responders, from transportation and logistics to food and agriculture. All depend on the Level 1 infrastructures.

The open door comes from a traditional culture of unrestricted public access. This openness traditionally flourishes because public and investor-owned utilities must answer to a demanding public, ratepayers, and various regulatory agencies. Even when these infrastructure stewards have critical assets to protect, when it comes to their public customers, they cannot be perceived as having something to hide. In this environment, defenses against infiltrators or any type of insider threat require a cultural shift. The challenge is to close the door to infiltrators while leaving it open to legitimate workers.

Even if an infiltrator sets sights on a worthy infrastructure target and exploits weak defenses, he or she still needs a dark corner free of oversight or restraint in order to gather pre-strike intelligence and then initiate an attack without risk of timely intervention and defeat. The best way to defeat such an attack is to remove the dark corners.

Second, as previously mentioned, Americans have a penchant for relying on technology to solve problems. This tendency places a premium on depth, at the occasional expense of breadth. As a result, in addressing the insider threat to critical infrastructure, the tendency leaves us attempting to penetrate with the intensity and focus of a laser what we should be illuminating with a flashlight. No matter how deep the laser drills, it points to only a fragment of the entire picture. Caught in the laser's beam, a clever insider can mask or explain away hostile activities with relative impunity.

The No Dark Corners approach substitutes the flashlight of open team and employee engagement for the laser of limited and specialized monitoring of corporate sentinels working in secret. It represents a method of implementing layered defenses, particularly on the front lines of detection and intervention: where critical operations take place.

Despite generations of study, the insider threat remains alive. Infiltrators continue to pose a risk to critical infrastructure. There are no easy answers. No Dark Corners shows promise, however, as an approach that fills the gaps in traditional defenses. In so doing, this approach stands poised to deliver an important benefit for defenders: the victory of ownership over surprise.

APPENDIX A: THREE ROUNDS OF DELPHI QUESTIONS

The following materials were sent to Delphi respondents over the course of two months to solicit their thoughts as part of the insider threat study. An interval of at least two weeks separated each of the three rounds of Delphi questions.

A. DELPHI ROUND 1 QUESTIONS

1. What is an insider threat in your view? Are there different kinds of insider threat? Please elaborate.

2. What do you see or have you seen that is observable in insider tactics?

If it helps to think of specific cases, without revealing any confidential or sensitive details, please comment on these questions in relation to a significant case you have experienced:

3. What did the trust betrayer do and for what motives?

4. What caused the trust betrayer to be exposed?

5. What signs pointed the way to the exposure?

Any other comments or insights you would like to add.

B. DELPHI ROUND 2 QUESTIONS

Thank you for participating in this study, once again. This time, let me incorporate input that came out of the first round into the current round of questions. We begin with some common denominator observations for all of you to rate on a scale of 1–5, follow with six questions that encourage you to comment, and end with some scenario questions for your reaction.

PART I: Ratings

Please rate these questions according to whether you agree or disagree, so that I can tell whether I have captured ideas correctly from your previous input.

Rating Scale: 1 = strongly disagree, 2 = disagree, 3 = neutral or no strong position, 4 = agree, 5 = strongly. Feel free to add comments, particularly if I have missed something.

	Observation/Statement	Your Rating (1–5)	Remarks (optional)
A.	Insider threats are people who possess legitimate access and occupy a position of trust in or with the organization that they are targeting.		
B.	The hostile insider most dangerous to an organization is likely to display "beat the system" talk or behaviors.		
C.	He or she is likely to be secretive.		
D.	He or she is likely to demonstrate an excessively proprietary interest in the job, including working unpaid for long hours.		
E.	He or she is likely to hoard or withhold information from others.		
F.	He or she is likely to show signs of elitism, arrogance, or acting superior to others.		
G.	He or she may display unexplained changes in personality, mood, or conduct.		
H.	He or she may appear resentful, disgruntled, or anti-social.		
I.	He or she is often the picture of the perfect employee.		
J.	He or she gives the impression of wanting to get even.		
K.	He or she is constantly seeking power.		
L.	He or she uses words like "unfair" and "hostile workplace," particularly if a malicious whistle-blower.		
M.	He or she exhibits a decline in job performance.		

PART II: Questions for Your Reaction and Comment

1. Some pattern analysis software (www.tagcrowd.com) identified **unexplained anger** as a common indicator that often surfaced in your collective descriptions of insider threats. Did I capture this correctly? In other words, does this make sense to you? Please comment.

2. Similarly, random audits or investigations based on reported suspicions, or even just as a matter of due diligence, appeared to emerge as a consistently mentioned countermeasure for stopping an insider threat before it is too late. Do you agree? Does this make sense to you? Please comment.

3. One of you pointed out that the more dangerous threats are either people who are suffering personal distress and seeking relief (like those responsible for workplace violence), or those who are more goal-oriented and seeking victory (like saboteurs). Do you agree? Please comment.

4. Another of you suggested that the most dangerous insiders generally fall into one of three categories: embezzler-thief, saboteur, and shooter. In this model, the embezzler-thief and saboteur are planners, while the shooter is more likely to erupt with "no coherent plan beyond buying large quantities of ammunition before the violent deed." Is it useful to think of insider threats by rating them High, Medium, or Low across these three dimensions? Do you agree? Please comment.

5. Who would you worry more about as a **threat to other people**: the insider who erupts or the insider who plans? Why?

6. Who would you worry more about as a **threat to the institution**, as someone who can take down the entire enterprise or organization: the insider who erupts or the insider who plans? Why?

PART III: Scenarios and Related Questions

Finally, look at two hypothetical insiders, Herman and Edna. They represent composites of your previous inputs and are chosen to represent potentially serious insider threats. You'll see a little information about them, followed by some questions.

Both Herman and Edna work for the same government agency, the state lottery commission of a northeastern state in the U.S. This institution is co-located in a complex housing the offices of the governor and leaders of the state legislature, who participate actively in VIP events involving the lottery commission, particularly since it has become a reliable source of revenue to offset state fiscal pressures. You will find the descriptions of these employees incomplete, to leave room for your imagination and to reflect realistic information gaps that investigators and defenders face when initially encountering potential threats to their institutions.

Two Employees of State Lottery Commission

HERMAN	EDNA
--18-year employee of State Lottery Commission --Competent in his area but passed over for promotions for last 7 years --Works uncompensated long hours and weekends --Very jealous of his turf and prerogatives --Hoards information, likes to be sole expert in his area --Bristles when questioned about his area, generally browbeats auditors with jargon and younger, timid supervisors into leaving him alone --Gives surface impression of ideal employee, but heard berating upper management in cafeteria and other informal settings --Rumored to have been involved somehow in involuntary transfer of one supervisor and in unexpected resignation of another because of allegations of discrimination that were not conclusively proven	--18-year employee of State Lottery Commission --Average worker but attendance and performance in decline during past 6 months --Overheard complaining about being sued by former partner for unpaid child support --Changed work location after ridicule by two co-workers, one a former sexual partner who has since filed 3 grievances and 1 ADA complaint against her --Repeatedly asked supervisor for overtime opportunities in order to pay for her mother's dialysis treatments --In last month, reported petty theft and vandalizing of her desk --Found her car "keyed" in employee parking lot before it was repossessed 2 weeks ago --Avoids her supervisor and no longer eats lunch in cafeteria --Is currently in process of having her wages garnished for unpaid child support as result of former domestic partner winning judgment against her in court

1. Which of these employees do you rate as potentially more dangerous to co-workers?

2. Which do you rate as a greater potential danger to the institution?

3. You just received a tip that one or both of these employees may be involved in some unauthorized activity that constitutes a threat to the State Lottery Commission or its staff. Who would you judge to be more likely to be involved in the following, Herman or Edna?

A. An attack of workplace violence that targets the payroll manager, a supervisor, and two co-workers.

B. A complex fraud scheme, undetected for years, that redirects a fraction of a penny spent on purchases of multiple lottery tickets. The funds go to an offshore bank account and, depending on the extent of the losses and negative press, the revelation could threaten the survival of the state's lottery system.

C. Compromise of insider details of a VIP event to a group of extremists operating as a nonprofit corporation that has been suspected of planning to assassinate the governor as a political statement.

D. Join an activist group through the Internet and, after being befriended by them at after-hours meetings and social events over a period of 18 months, offer to provide information that will allow insider access during an upcoming ribbon-cutting ceremony where the governor and several state government and business executives will be in attendance.

Comments on any or all of the above:

C. DELPHI ROUND 3 QUESTIONS

Thank you for your continued participation. Through your responses and comments, you have provided useful insights on indicators of insider threats, as well as ideas on how to stop them. You will find a one-page summary of highlights from the last round in Attachment 1. Some of you wanted to know how your answers corresponded with others, hence more detailed diagrams summarizing the findings in Attachment 2. Both attachments are purely optional, for perusal at your convenience.

You have all been very gracious and generous with your replies, so I hope this final round will be less demanding and a little fun. Please respond in two weeks.

We now focus on countermeasures. There is only one rating question, and an opportunity to unleash your imagination in tackling one problem. Now, you are the opposition. Think like a terrorist for the rating question and your attending comments.

Your Task: Attack one of these critical infrastructure targets (your choice): water, electricity, or telecommunications utility. (Dr. Ted Lewis, author of *Critical Infrastructure Protection in Homeland Security* and one of my instructors, rates these as Tier 1 critical infrastructures because of their capacity for influencing cascading failures among the rest.)

Your Method: Infiltrate one of these infrastructure stewards (i.e. a public sector or private sector utility) or recruit an agent from within the utility to inflict maximum damage directly or by supplying invaluable information and access to your attack cell, which will do the dirty work.

Your Timing: 6 months – 8 years (This is based on two things. One is the interval between attacks on the World Trade Center. Another is an al Qaeda operative quote by Richard Miniter in *Losing Bin Laden* (Washington D.C.: Regnery Publishing, 2003, p. 95) which highlighted the willingness to lie in wait. Early in his training, an al Qaeda operative … recalls repeatedly chanting this Koranic verse: “I will be patient until patience is worn out from patience.”

Rating Question

Please rate these countermeasures according to which you would consider the most challenging if planning to attack a critical infrastructure target from within. You will see the countermeasures described briefly below, with room for your ratings next to them.

Rating Scale: 1 = no obstacle, 2 = easily overcome, 3 = problem but surmountable with average planning and resources, 4 = significant hurdle but surmountable with considerable effort and resources, 5 = significant hurdle and possibly insurmountable.

COUNTERMEASURES

A. **Brother's Keeper** option that encourages co-workers to identify and act on suspicions of hostile or inexplicable insider activities. This could even be similar to acting on reasonable suspicion to report a substance abuse problem at work. RATING (1–5): _____

B. **No Dark Corners** option, or no alone zone, that configures work in a way that aims to reduce chances for a sole individual working in a sensitive area undetected, with either another trusted employee within line of sight or some form of remote surveillance or detection creating the possibility that someone may be watching. Some of you have seen this in the defense or nuclear security industry. RATING (1–5): _____

C. **Random Audits** option, which could be operational, process, financial audits or any combination that would potentially uncover evidence of hostile activity. RATING (1–5): _____

D. **Technology-Based Monitoring** option, which would involve automated controls and alarms that annunciate or terminate access and generate exception reports whenever an employee attempts to gain unauthorized access or exceeds a defined number of authorized queries and transactions in a sensitive area. RATING (1–5): _____

E. **Background Investigations or Updates** option, which involves screening of new hires and possible periodic update investigations of existing employees. RATING (1–5): _____

F. **Sting or Dangle Operations** option, which involves flushing out hostile insiders by pretext and could include luring a hostile insider to join what purports to be a terrorist organization that does not really exist or having a trusted insider exhibit behaviors that give the appearance of being an excellent recruitment target for you to cultivate, not realizing that this is a double agent. RATING (1–5): _____

G. **Other**: your own idea or ideas that do not fit into the options above and would rate at least a

4. RATING (1–5): _____

TASK: Which infrastructure did you select as your target (water, electricity, or telecommunications utility)? Why?

METHOD: Which method did you select (infiltrating with your own operative, or recruiting an agent already there)? Why? If you recruited someone already in place, what is the most you expect this person to do for you? COMMENTS on ratings, countermeasures, or your own thoughts about how you would conduct an attack and what would stop you:

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SUMMARY OF DELPHI ROUND 1 FINDINGS ACCOMPANYING ROUND 2 QUESTIONS

Thoughts from Delphi Round 1

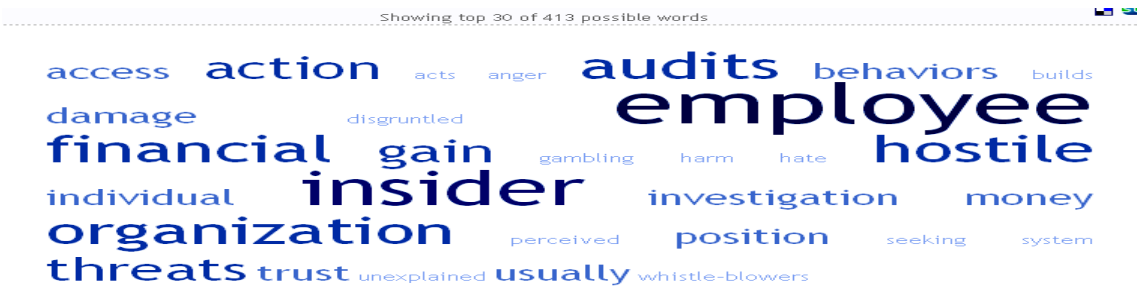
For those of you able to review this information, here is some preliminary analysis of responses to the first round of questions in the Delphi survey on the insider threat. The next round will focus on telltale signs or indicators (aka traplines). The final round will focus on countermeasures (aka tripwires).

These were some of the more interesting insights that surfaced:

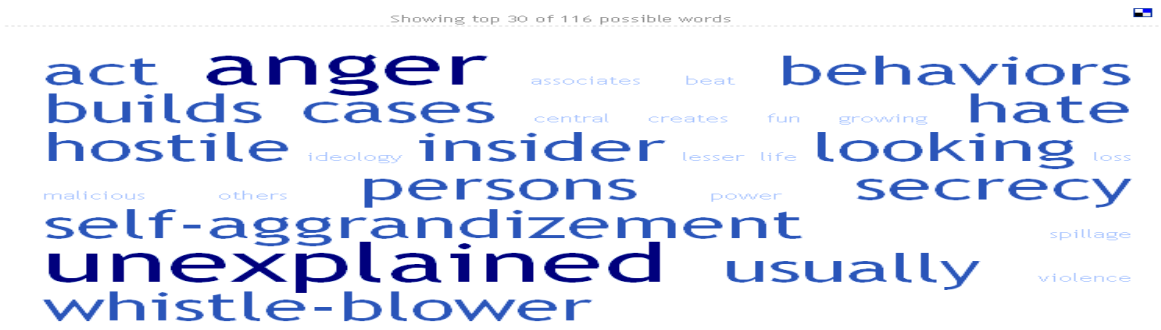
- Conversational spillage/inexplicably hostile behavior, own disclosure
- "Beat the system" talk, behaviors; rumors and suspicions reported to management and then investigated; greatest loss from insider at highest level
- Sick fun; frequent rotations, good auditing
- Getting even a central theme
- Reduce discoverability; decline in performance; visible anti-social behaviors. "Sudden" anomalies usually have precursors that supervisors don't act on.
- Persons who hate are usually outspoken about it.
- Unexplained changes of personality, mood, or conduct; unexplained money, family life, outside associates. Every advance in technology creates new vulnerabilities.
- Always exploits the organization's weakness. Deterred only by strong chance of discovery and swift punishment. Insider is never observed as a threat, employs secrecy, often the picture of the perfect employee. Whistle-blower.
- Self-aggrandizement. Ideology may play a lesser role in corporate cases but is primary in a terrorist scenario.
- Elitism or anger and aggression; considers others inferior. Expressed hate and anger. Secrecy, self-aggrandizement; growing hostility, unexplained anger.
- Constantly seeking power, dismissive of victim(s)
- For cases of violence, not sneaky but stewing in own myopic juices. Malicious whistle-blower slowly builds up a body of questionable documentation. A shooter acts alone and is looking for relief and can often be guileless. An internal saboteur is looking for victory and builds up to an attack.

In addition to looking for common themes and unique observations, I used a tool called Tag Crowd to make some patterns more visually obvious. This visual analysis of survey data is available at http://www.tagcrowd.com at no cost for individual and educational uses, thanks to Daniel Steinbock, a doctoral student at Stanford University. The output itself is called a text cloud, which is also referred to as a tag cloud. You will see two of these on the next page.

Text Cloud Showing Frequency of Words in Summary of Responses



Text Cloud Showing Frequency of Words Appearing in Subset of More Interesting Insights



Analysis

The first text cloud compilation and sorting of overall responses, highlights observations and themes common to the insider threat writ large, i.e., the insider as an employee, often motivated by financial gain, operating in an organization, and subject to being given away by actions, audits, and behaviors.

The second text cloud, concentrating exclusively on the more telling remarks of respondents, begins to lend greater granularity to the first image. More indicators begin to surface, with the most telling summarized as unexplained anger, the two most prominent words in the text cloud. Other themes emerge as potentially revealing indicators, such as tendencies of self-aggrandizement and

secrecy among hostile insiders, which offer possibilities for detection when tied to corresponding traits and behaviors. Interestingly, “whistle-blower” appears in both the more general text cloud and the more sharply focused one. Respondents with backgrounds in the worlds of corporate fraud investigations, intelligence, and clinical assessment of workplace violence threats independently converged on the notion that malicious whistle-blowers are beginning to emerge as nascent saboteurs. It is equally interesting to note that money and financial gain, which were prominent in Figure 1, are absent from Figure 2. One respondent indirectly offered the reason for this omission by noting that the most destructive damage is rarely driven purely by a desire for financial gain.

The foregoing use of text clouds fell short of supporting the investigator’s preliminary sense of emerging distinctions in attempting to divide insider threats into overly restrictive and artificial categories. Consequently, the preliminary categorization effort postulating the existence of a spectrum of trust betrayers found insufficient traction to survive closer scrutiny. However, thanks to the text cloud analysis and the further, iterative study of responses that this analysis inspired, a dichotomy began to emerge and formulate the basis for Delphi Round 2 inquiries.

Specifically, is there value in broadly categorizing insider threats in terms of whether they plan their attacks? Evidence of planning corresponds to the insight of a behaviorist who noted that the saboteur’s objective is seeking victory. By contrast, a dearth of planning that could instead present itself as an eruption corresponds to what the same respondent called the shooter’s objective of seeking relief. Pursuing such a dichotomy further also offers value in that it creates nesting areas for the different types of cases already cited by the respondents while offering a simpler, more intuitive way of drawing distinctions and seeking corresponding behavioral signatures that could give away malicious insiders before they carry out their attacks. Thus, this new tentative categorization forms the basis not only for further questions but for formulation of two different kinds of insider threat scenario to now structure respondent thinking along common denominators without pre-ordaining responses.

As Delphi Round 2 begins to sharpen the focus on traplines, that is, on the behavioral signatures and other indicators that will assist defenders in identifying hostile insiders, Table 3 offers a framework for distinguishing the insider threats who can be fatal to an institution from those whose potential lethality is largely restricted to individuals.

Table 3: Proposed Insider Threat Dichotomy

THOSE WHO PLAN	THOSE WHO ERUPT
More dangerous to institution	More dangerous to individual(s)
Seek victory	Seek relief
More meticulous, analytical, secretive, subtle, deceptive	Guileless, self-revealing
Target the institution	Target individual or individuals perceived to be causing them distress
Ideologically oriented or entirely mercenary	Victimized or self-described as victimized or wronged
Dismissive of victims, angry at them, acts superior to them	Dismissive of victims, angry at them, acts as if unfairly treated by them
Exploits organization's weaknesses	Exploits organizational weaknesses
Picture of the perfect employee	Declining performance
Self-aggrandizing, self-enriching, in control	Territorial, turf conscious, losing control
Getting even, disgruntled	Getting justice, disgruntled
Saboteur, Sleeper, Traitor	Desperate employee

APPENDIX C. SUMMARY OF DELPHI ROUND 2 FINDINGS ACCOMPANYING ROUND 3 QUESTIONS

Highlights of Delphi Round 2

Part I

	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE	
A			58%	42%	Definition
B	17%	42%	33%	8%	Beat the system
C	8%	42%	17%	33%	Secretive
D	8%	17%	58%	17%	Owns the job
E		33%	33%	33%	Withholds info
F	8%	25%	25%	42%	Arrogant, elitist
G		25%	33%	42%	Unexplained changes
H		8%	67%	25%	Resentful
I	17%	42%	42%		"Perfect" employee
J	8%	50%	42%		Getting even
K	33%	42%		25%	Seeking power
L		42%	50%	8%	Says "unfair"
M	25%	42%	33%		Work declines

Part II

Most Useful Distinctions: unexplained anger as common indicator, random audits as strong countermeasure, and planner as insider most dangerous to institution.

Part III

Planner is more dangerous, more prone to complex fraud. But planner could also do more physical harm than insider who erupts. Also, planner may not be a joiner, hence not as likely to join a group or react well to handlers.

Overall

Some themes where there was strong convergence:

- Indicators of unexplained changes in behavior and in resentful or disgruntled presentation of the hostile insider.

- Secondary indicators of the hostile insider exercising overly proprietary interest in the job, expressing a perception of unfair treatment, and appearing arrogant or elitist.
-

- Random audit as a good, if not the best, countermeasure

- The planner as the bigger threat to the institution, with some distinctions offered in remarks to the effect that a workplace violence attack, or rage killing, might constitute a personal tragedy for those victimized but was not an existential threat to the institution.

Other themes which showed early promise in surfacing useful distinctions for further probing ended up being dry holes. Some of these:

- The insider as one who withholds information. Respondents suggested that this might be true enough but was often difficult if not impossible to gauge until after the fact, hence of limited predictive value.

- Seeking power, being secretive, and exhibiting decline in performance also proved to be nonstarters. Clarifying comments explained that some of these traits were equally visible elsewhere, hence of limited value in trying to uncover hostile insiders. One respondent reasoned that ambitious competitors could easily seek power without becoming insider threats. Similarly, another respondent noted that, in his experience with traitors, once they had embarked upon a plan for stealing secrets to pass to a foreign power, they tended to level off in their outward ambitions and general performance. Evidently, this is to avoid inviting scrutiny while, at the same time, concentrate their energies on their clandestine endeavors.

- Efforts at categorization, whether as an insider seeking victory vs. relief, or as belonging to one of three classes (embezzler-thief, saboteur, or shooter (rage killer/workplace violence perpetrator) also went nowhere. Parts of these were negated by the very respondents who first suggested them. Evidently, there is just too much variation in views and in real cases to permit ready categorization along these lines.

APPENDIX D. EXPERT COMMENTS AND STORIES

Delphi respondents included a number of remarks and stories that went beyond their responses to specific questions. Select examples that illustrate or supplement other research findings appear below.

A. TRANSPARENCY: PUSHING OUT MANAGEMENT DATA

When they first started becoming available, and some time afterwards, management reports were pretty restricted. The idea was that it took a lot of work to produce them. They contained inside information that could be embarrassing to some people or could even increase liability if in the wrong hands. The trouble was, that the reports only went to top managers, and any good top manager lacked the extra time necessary to break down the reports and study them at length to compare against employee and work unit performance. Sure, spot checks were possible. I tried those. But, they remained pretty much hit and miss. No one could spot check every operation, and it seemed unfair to single out only the ones within reach.

One day, I looked at a stack of attendance reports, budget variances, analysis of problems we had experienced with some expensive equipment, overtime statistics, and other such things that were piling up on my credenza. Realizing I would never have time to go through them all before my secretary ultimately filed or tossed them, I decided I either had to find a way for getting value out of them or taking my name off distribution. So, I broke them down and pushed them out to the front-line managers responsible for their various work units and teams. Guess what? They were the best people to get the reports. Why? Because they recognized every person and line item mentioned, knew instinctively what was working and what was out of line, and welcomed the chance to use them to keep score. It saved me a lot of work and put the right yardstick in the hands of the people who needed to measure in inches and feet every month the kinds of things I could only afford to look at in miles and on a

quarterly basis. Besides, their own teams started looking forward to the details to know how well they did compared to another team at a different plant or compared to their own performance a year ago.

A great example was overtime. By parceling out OT reports to each manager and team, we saved $1.5 million the first yea—just by looking through the eyes of the people closest to the affected areas. The same kind of cost savings occurred when we figured out how to do this with cellular telephone bills.

There is no substitute for displaying results for everyone to see. This is what makes metrics meaningful. Otherwise, employees treat what you are telling them like just an opinion.

B TWO-PERSON RULE

It used to be called the two-man rule, or the two-person-integrity rule. According to one classified program's description of how this works, the rule is designed to bar access to a sensitive area or asset by any lone individual. Two authorized employees are considered present when they are physically in a position where they can positively identify use of unauthorized procedures in relation to the operation at hand. The two-person team must be knowledgeable of safety and security requirements and both individuals must be present during any activity requiring access to sensitive areas or equipment. Each of the two is responsible for enforcing the two-person rule at all times while in the sensitive area where the rule applies.

C. A BUSINESS DECISION TO FAVOR INFILTRATORS

I would not target an insider already in place because the task of identifying an appropriate and vulnerable employee who could be recruited is too difficult, and failure would compromise my program.

One way to insulate the attack from compromise is to keep the infiltrator unaware of the ultimate objective. This could also help the infiltrator pass a background check, particularly if the details of the operation were spectacular

enough to make him nervous, if he were aware of them. His time on the job would be spent figuring how to bypass technical countermeasures. He would act "normal," fit in, and be part of the team.

D. SMALL WORLD INSIDER CHALLENGES

Recruiting an agent is impossible in small town environments or small utilities where the locals all know each other intimately. In many ways, these environments create a degree of transparency that becomes lifelong and remains very insular. Outsiders spend years trying to achieve the same level of trust that is automatically conferred to Bobby Joe's grandson who is also the nephew of Rita Sue, the mayor's sister. In these places, infiltration is most effective via contractors.

Contract employees in place for extended periods of construction tend to be unescorted and gain unlimited access to critical areas because there is nobody to watch them. Companies often employ non-English speaking workers who are faceless and interchangeable in their eyes, as long as they can meet the requirements of hard labor associated with construction work.

E. WHY NO "BROKEN WINDOWS" IN INFRASTRUCTURE DEFENSE

The reasons we have not extended these concepts from protecting communities to institutions and infrastructure are that we assume infrastructure is under private control. So, it becomes someone else's problem. Also, the traditional labor-management and public right-to-know pressures have dominated in the boardroom and in regulatory decision-making environments, thereby reducing the market for or receptivity to such concepts. Moreover, when there is success in altering the culture of these institutions, the victories tend to be attributed to and monopolized by the founder or chief executive. In reality, whether it is a teacher presiding in a classroom or a cop maintaining order on the streets of the precinct, or a Fortune 500 CEO bringing a company back from the

brink of bankruptcy—no one does it alone. This achievement requires a sense of ownership on the part of all the people on the team. With it, amazing things happen. Without it, even mediocrity may remain out of reach.

LIST OF REFERENCES

Allen, T. B., & Polmar, N. (1988). *Merchants of treason: America's secrets for sale.* NY: Delacorte Press.

Anderson, M. (1994). Introduction. In T. Sarbin, R. Carney, &. C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal* (pp. 1–17). Westport, CT: Praeger.

Ben-Yehuda, N. (2001). *Betrayals and treason: Violations of trust and loyalty.* Cambridge, MA: Westview.

Brackney, R. C., & Anderson, R. H. (2004). *Understanding the insider threat.* Santa Monica, CA: RAND Corporation. Retrieved August 14, 2008 from http://www.rand.org/pubs/conf_proceedings/CF196/index.html

Business Dictionary.com. Retrieved July 4, 2009 from http://www.businessdictionary.com/definition/management-by-exception-MBE.html

Carney, R. M. (1994). The enemy within. In T. Sarbin, R. Carney, &. C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal* (pp. 19–38). Westport, CT: Praeger.

Covey, S. M. R., & Merrill, R. R. (2008). *The speed of trust: The one thing that changes everything*. New York: Free Press.

Day, R. (2009, June). Remotely monitored CCTV reduces theft by 80%. In *Secure Times.* Essex, UK: Sheen Publishing, Ltd.

Equal Employment Opportunity Commission. (2009). *Employment tests and selection procedures.* Retrieved May 8, 2009 from http://www.eeoc.gov/policy/docs/factemployment_procedures.html

Eoyang, C. (1994). Models of espionage. In T. Sarbin, R. Carney, &. C. Eoyang (Eds.), *Citizen espionage: Studies in trust and betrayal* (pp. 69–91). Westport, CT: Praeger.

Fein, R., B., & Vossekuil, B. (1998). *Protective intelligence and threat assessment investigations.* Washington, DC: National Institute of Justice.

Fernandez-Araoz, C., Groysberg, B., & Nohria, N. (2009, May) The definitive guide to recruitment in good times and bad. *Harvard Business Review*, pp. 74–84.

Fishman, J. J. (2007). *The faithless fiduciary and the elusive quest for nonprofit accountability.* Durham, NC: Carolina Academic Press.

Herbig, K. L. (2008, March). Changes in espionage by Americans: 1947–2007. *Technical Report 08–05* . Monterey, California: Defense Personnel Security Research Center.

Hollywood, J., Snyder, D., McKay, K., & Boon, J. (2004). *Out of the ordinary: Finding hidden threats by analyzing unusual behavior*. Santa Monica, California: RAND Corporation.

ICE Mutual Agreement for Government and Employers. (2009, March 2). U.S. Immigrations and Customs Enforcement. Retrieved May 29, 2009 from http://www.ice.gov/partners/opaimage/image_faq.htm

Johnson, C. Y. (2009, February 8). Breakthrough on "broken windows." *Boston Globe*. Retrieved July 5, 2009 from http://www.boston.com/news/local/massachusetts/articles/2009/02/08/breakthrough_on_broken_windows/?page=2

Kaupla, J. (2008, May 25). Are you hiring future champions or future saboteurs? *ERE.net* (recruiters' network). Retrieved August 24, 2008 from http://www.ere.net/2008/03/25/are-you-hiring-future-champions-or-future-saboteurs/

Kelling, G. L., & Coles, C. M. (1996). *Fixing broken windows: Restoring order and reducing crime in our communities.* New York: Touchstone.

Kim, W. C., & Mauborgne, R. (2005). *Blue ocean strategy*. Boston, MA: Harvard Business School Press.

Kowalski, E., Cappelli, D., & Moore, A. (2008, January). *Insider threat study: Illicit cyber activity in the information technology and telecommunications sector.* Pittsburgh, PA: U.S. Secret Service and Carnegie Mellon Software Engineering Institute, pp. 24–26.

Leonard, D. & Swap, W. (2004, September) Deep smarts. *Harvard Business Review.* Retrieved July 29, 2008 from http://harvardbusinessonline.hbsp.harvard.edu/hbsp/hbr/articles/article.jsp?ml_action=getarticle&articleID=R0409F&pageNumber=1&ml_subscriber=true&uid=24509483&aid=R0409F&rid=24600531&eom=1

Levitt, S. D. & Dubner, S. J. (2005). *Freakonomics: A rogue economist explores the hidden side of everything*. New York, NY: HarperCollins.

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security.* Hoboken, New Jersey: John Wiley & Sons.

Merriam-Webster Online Dictionary. (2009). Retrieved July 9, 2009, from http://www.merriam-webster.com/dictionary/copilot

Murphy, P. (1999). Surveillance. In *Security business practices reference, volume 2.* Alexandria, VA: American Society for Industrial Security.

Newman, O. (1972). *Defensible space: Crime prevention through urban design.* New York: Macmillan Publishing Company.

Nieto, M., Johnston-Dodds, K., & Simmons, C. W. (2002). *Public and private applications of video surveillance and biometric technologies.* California Research Bureau. Sacramento: California State Library Foundation.

Noonan, T., & Archuleta, E. (2008, April 6). *The insider threat to critical infrastructures.* The National Infrastructure Advisory Council.

Olson, D. T. (2005). The path to terrorist violence: A threat assessment model for radical groups at risk of escalation to acts of terrorism. Master's thesis, Naval Postgraduate School, Monterey, CA. Retrieved September 5, 2008 from https://www.hsdl.org/homesec/docs/theses/05Sep_Olson.pdf&code=08ed3b0e4d34e346e2dc3540cdc0e1f8

Peters, T. (2007, September 25). Speech on emerging security trends. Keynote address presented at the 2007 seminar and exhibits, American Society for Industrial Security, Las Vegas, NV.

Pre-employment Background Screening Guideline. (2006). American Society for Industrial Security, International. Retrieved June 6, 2009, from http://www.asisonline.org/guidelines/guidelinespre-employ.pdf

Protection of Assets Manual. (2006). Arlington: American Society for Industrial Security, International. Volume II of IV, pp. 1–IV–1 to 1–IV–18.

Puleo, A. J. (2006). *Mitigating insider threat using human behavior influence models.* Master's thesis, Air Force Institute of Technology, Wright-Patterson AFB, OH.

Shaw, E. D. & Fischer, L. F. (2005). *Ten tales of betrayal: The threat to corporate infrastructures by information technology insiders.* Monterey, CA: Defense Personnel Security Research Center. Retrieved September 6, 2008 from https://www.hsdl.org/homesec/docs/dod/nps33-122107-01.pdf&code=cabcfb03c46e06e36ad177e692594c28

Sims, J. E. (2005). Understanding ourselves. In J. E. Sims & B. Gerber, (Eds.) *Transforming U.S. intelligence*. Washington: Georgetown University Press.

Skulmoski, G. J., Harman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education , 6* . Retrieved November 23, 2008 from http://jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf

U.S. Congress, Office of Technology Assessment. (1990, June). *Physical vulnerability of electric system to natural disasters and sabotage, OTA-E-453.* Washington, DC: U.S. Government Printing Office.

Wilber, D. Q., & Sheridan, M. B. (2009, June 6). State Department Retiree Accused of Spying. *Washington Post*. Retrieved June 6, 2009 from http://www.washingtonpost.com/wp-dyn/content/article/2009/06/05/AR2009060502359_pf.html.

Wilson, J. Q., & Kelling, G. L. (1982, March). Fixing broken windows. *The Atlantic Monthly.*

Wright, P. (1987). *Spycatcher: The candid autobiography of a senior intelligence officer*. New York: Viking.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Shane Chapman, Assistant Manager, Water System Operations
   Metropolitan Water District of Southern California
   Los Angeles, California

4. Kim Corthell, Fellow
   Homeland Security Studies and Analysis Institute
   Arlington, Virginia

5. Don Boland, Executive Director
   California Utilities Emergency Association
   Mather, California